POLITECNICO DI TORINO

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea Magistrale

# Analisi normativa e applicazione pratica della firma elettronica avanzata


**Relatori:**
prof. Antonio Lioy
prof. Marco Mezzalama

**Candidato:**
Alessandro Avila

**ECM Unit Manager**
**Consoft Sistemi S.p.A.**
dott. Fulvio Guglielmelli

Anno accademico 2012-2013

# Sommario

Il tema principale che muove l'intera trattazione dell'elaborato di tesi è quello relativo al concetto di firma elettronica, più precisamente di firma elettronica avanzata (abbreviata in FEA), apposta ad un documento informatico, componente basilare (nonché primario) nel processo di digitalizzazione e conservazione del documento, che ha avuto una evoluzione significativa nel tempo e che solo in questi ultimi anni vediamo emergere come nuova tecnologia (o meglio, come nuovo processo) sostenuta da un sistema normativo riconosciuto a livello internazionale ma ancora soggetto a revisioni e mutamenti.

Individuato quindi il contesto principale nel primo capitolo, il successivo affronta la formazione del sistema normativo ed italiano (in particolar modo) in materia di firme elettroniche, dedicando, nello specifico, ampio spazio all'analisi delle loro diverse declinazioni (firme semplici, firme avanzate, firme qualificate, ecc.) e dei differenti effetti giuridici e risvolti legali che comporta il loro utilizzo.

Focalizzata l'attenzione sulla normativa in materia di FEA, viene proposta una disamina dei principali campi di applicazione e delle tecnologie crittografiche di base che ne regolano il funzionamento; tema di particolare interesse è quello delle tecnologie biometriche applicate al processo di firma, che godono di una certa popolarità ed utilità in tutti quegli ambiti in cui l'apposizione di una firma è una prassi frequente; la biometrica di firma ha permesso la nascita di nuovi scenari applicativi (in primis quello della firma su tablet elettronico anziché su foglio di carta), senza richiedere un cambio di abitudini da parte dell'utente e mantenendo certi standard di sicurezza e privatezza dei dati.

La seconda parte dell'elaborato verte essenzialmente sull'analisi e la progettazione di una soluzione applicativa di FEA; viene anzitutto offerta una panoramica generale dei principali strumenti software (SDK, Software Development Kit) adottati per la realizzazione di una applicazione client stand-alone in ambito desktop, nonché dei principali dispositivi di firma con cui l'utente potrà interagire; la discussione si concentrerà poi sull'analisi delle classi, delle funzioni e delle librerie utilizzate per gli scopi previsti, quindi sulla descrizione dei moduli, delle interfacce e delle strutture dati del programma.

Sulla base di quanto esposto precedentemente, seguirà la trattazione di processo vero e proprio di firma, illustrando un tipico esempio di utilizzo dell'applicazione da parte di un utente firmatario: verranno mostrati i principali passi attraverso cui l'utente realizza l'apposizione, su un documento, di una firma acquisita da dispositivo esterno, dopo aver impostato alcuni parametri di configurazione della firma stessa.

Infine il capitolo conclusivo propone una serie di considerazioni finali sull'introduzione della biometria nelle nuove realtà applicative (trasferimento dei dati biometrici, trattamento dei dati personali, criticità del dato biometrico, ecc.), che possono dare seguito a possibili sviluppi futuri della soluzione qui presentata.

# Ringraziamenti

Ringrazio sentitamente anzitutto il relatore referente del Politecnico di Torino, professor Antonio Lioy, per aver seguito l'avanzamento della composizione della tesi con attenzione e rigore, fornendomi periodicamente precise direttive sulle modifiche da apportare, senza il cui contributo la tesi non sarebbe risultata della stessa qualità tecnico-scientifica.

Inoltre, un ringraziamento dovuto va all'avvocato Annarita Ricci, dello studio legale Finocchiaro, per le preziose delucidazioni e direttive nel campo legislativo e giuridico delle firme elettroniche, senza le quali l'analisi normativa della prima parte dell'elaborato non avrebbe avuto lo stesso rigore tecnico.

Un ringraziamento speciale va alla dottoressa Cristina Bonino, presidente e amministratore delegato di Consoft Sistemi S.p.A., per avermi offerto l'opportunità di conoscere e vivere concretamente una realtà aziendale, nonché di acquisire quelle conoscenze ed esperienze professionali che mi sono servite poi nella scrittura dell'elaborato; vorrei infine esprimere la mia sincera gratitudine al dottor Fulvio Guglielmelli, mio relatore aziendale, per la possibilità di sviluppare la tesi su un tema così attuale e potenzialmente innovativo come quello delle firme elettroniche avanzate, sottolineando la sua particolare disponibilità a chiarimenti e dedizione durante la stesura di questo lavoro.

# Indice

# Capitolo 1

# Introduzione

## 1.1 Il documento informatico: dematerializzazione e conservazione

L'archiviazione informatica dei documenti è un obiettivo prossimo a compiersi e, grazie alle odierne tecnologie, ancor più che in passato. La gestione tradizionale del documento cartaceo risulta ormai particolarmente dispendiosa dal punto di vista economico-amministrativo e porta con sé una serie di aspetti negativi: difficoltà di condivisione, di ricerca, scarsa capacità di garantirne l'integrità nel tempo, ecc.

Affinché il processo di **dematerializzazione** (o digitalizzazione, intendendosi con ciò la realizzazione di prodotti che siano originariamente e completamente informatici) giunga al suo completamento e produca risultati pratici ulteriori rispetto alla semplice eliminazione del cartaceo (basti pensare, ad esempio, all'incremento di efficienza e alla riduzione dei costi), è tuttavia necessario ridefinirne o migliorarne alcuni punti, sia sul piano normativo che su quello relativo all'individuazione di modelli organizzativi innovativi ed efficienti.

Poiché il sistema giuridico italiano fonda una parte consistente del processo amministrativo sul valore legale del documento, è indispensabile che, nella procedura che segna il passaggio dal documento cartaceo al documento digitalizzato (ossia il documento informatico), venga garantita la caratteristica probatoria del documento stesso. Le difficoltà implementative delle tecnologie

Figura 1.1. Archiviazione digitale dei documenti.

finalizzate ad automatizzare la procedura informatica e le resistenze culturali ne hanno rallentato lo sviluppo nel tempo: dobbiamo infatti riconoscere che siamo di fronte ad una profonda rivoluzione non solo giuridica, ma anche culturale, che svincola il documento dal supporto fisico che lo

ha contraddistinto per secoli, la carta per l'appunto (e prima di questa la pergamena e la pietra); tuttavia, la rapida diffusione dei mezzi di comunicazione digitali, globalmente connessi alla rete Internet e di conseguenza l'esigenza crescente dello scambio di documenti digitali tra utenti fisicamente distanti tra loro, la pongono come fenomeno appartenente alla realtà quotidiana ed appare quindi necessaria la costituzione di un modello giuridico, amministrativo ed organizzativo che tenga in considerazione tali istanze [1].

La sottoscrizione dei documenti, operazione fondamentale (nonché primaria) della procedura di archiviazione informatica, di fatto costituisce l'applicazione principale in vista della quale si fonda l'intera struttura normativo-giuridica che riguarda la **firma elettronica**: ponendosi nell'ottica di archiviare digitalmente un documento o inoltrarlo per via telematica, questo viene prima firmato elettronicamente. L'introduzione della firma elettronica rappresenta il tassello necessario nel percorso che ha come obiettivo la semplificazione dei processi amministrativi dello Stato: questo strumento sta assumendo un'importanza sempre più rilevante, grazie anche ad una gestione documentale sempre più digitalizzata; esso consente di facilitare lo scambio di informazioni, proteggerne l'integrità nel tempo e l'appartenenza ad uno specifico proprietario (sia esso una persona fisica o un ente giuridico).

I processi mutano, le tecnologie evolvono e si diversificano, rispondendo a nuove esigenze; per questo motivo anche le firme elettroniche hanno subito in quest'ultimo decennio il susseguirsi di varie trasformazioni, adattamenti normativi e, complice la mancanza di un coordinamento sistematico a livello internazionale, la realizzazione di una molteplicità di tipi di firme informatiche, con caratteristiche giuridiche e di sicurezza ben distinte. Le recenti novità in materia di amministrazione digitale lasciano supporre che la vicenda sulla "innovazione legislativa" sia destinata a proseguire.

## 1.2 Obiettivi della tesi

Tra i propositi che muovono lo sviluppo di questa tesi vi è sicuramente l'esigenza di fornire una visione chiara e completa del concetto di firma informatica, apposta ad un documento informatico, più precisamente firma elettronica e firma elettronica avanzata, componenti principali nel processo di digitalizzazione e conservazione del documento, che hanno avuto un'evoluzione significativa nel tempo e che solo in questi anni vediamo emergere come nuova tecnologia (o meglio, come nuovo processo) sostenuta da un sistema normativo riconosciuto a livello internazionale ma ancora soggetto a profonde revisioni e mutamenti.

Individuato il contesto normativo che regola le firme elettroniche avanzate, concentreremo la nostra attenzione sui principali campi di applicazione e sulle diverse declinazioni delle firme avanzate nei vari processi di business; particolare importanza verrà dedicata all'analisi delle tecnologie biometriche e quindi delle firme grafometriche, componenti essenziali nei nuovi processi di firma.

Verrà in seguito svolta l'analisi, la progettazione e l'implementazione di una soluzione applicativa di firma elettronica avanzata, sviluppata in ambito desktop e basata sui concetti espressi nel corso della trattazione.

La tesi è stata svolta presso la società Consoft Sistemi S.p.A., di cui viene fornita una breve descrizione nella sezione seguente.

### 1.2.1 Consoft Sistemi S.p.A.

Consoft Sistemi è un'azienda italiana presente sul mercato dell'ICT[1] dal 1986 con sedi a Torino, Milano, Genova, Roma e Tunisi, 400 dipendenti ed un fatturato di circa 22 milioni di Euro.

[1] Information and Communication Technology.

Accanto alla capogruppo Consoft Sistemi sono attive altre tre società: *Consoft Consulting*, che fornisce consulenza strategica, operativa e tecnologica su piattaforma SAP, *CSdomotica*, specializzata in tecnologie legate all'automazione di edifici domestici e industriali ed ai cablaggi strutturati, *Consoft Sistemi MEA*, per espandere l'offerta della capogruppo, in particolare quella legata alle Telecom, nel mercato nord-africano e medio-orientale.

Consoft Sistemi ha focalizzato la propria offerta su sei aree tematiche nell'ambito delle quali è in grado di realizzare soluzioni "end to end" per i propri Clienti attraverso attività di consulenza, formazione, system integration e managed services.

**IT Governance & Management**

Per un allineamento ed ottimizzazione dei servizi IT alle necessità aziendali. L'offerta ITG&M abbina competenze metodologiche e consulenziali certificate con la fornitura di strumenti software per supportare i clienti nelle attività di pianificazione, progettazione, implementazione, gestione e controllo delle infrastrutture IT. Le attività vengono svolte nel rispetto delle Metodologie e delle Regolamentazioni ITIL, BS7799, Cobit, ISO 9000. Le aree principali sono Application & System management, Application Performance Management, Capacity Management, Networking, Sicurezza, Compliance, supporto alla introduzione di metodologie ITIL. Consoft Sistemi ha stretto accordi di partnership con vendor internazionali leader per proporre soluzioni software innovative, di elevata qualità, in grado di contribuire alla riduzione dei costi di gestione e al miglioramento del servizio IT.

**Business Intelligence**

Per una gestione dell'informazione che possa contribuire alla creazione di valore per l'azienda, Consoft Sistemi ha integrato le proprie competenze tecnologiche sui processi di Business Intelligence (ETL, Data Modeling, Data Quality, Planning, Data Warehouse, ecc.) con quelle legate agli aspetti di business e di industry. Dall'offerta di soluzioni verticali di settore (customer segmentation, cost allocation, audience ratings, ecc.) ai servizi di gestione applicativa, dal disegno del modello logico alla scelta della soluzione tecnologica, allo sviluppo e all'implementazione di progetti complessi, Consoft Sistemi è in grado di supportare i propri clienti lungo tutte le fasi del ciclo di vita di una soluzione di Business Intelligence.

**Business Integration**

Per rendere le componenti ICT adattabili dinamicamente al business, Consoft Sistemi propone soluzioni architetturali multicanale e multipiattaforma, fondate sul modello SOA, che attribuiscono al processo di business un ruolo centrale. Nella fase di startup dei progetti Consoft Sistemi apporta valore aggiunto nella definizione di linee guida e best practice e mette a disposizione la consulenza specialistica. Tra le aree d'intervento: organizzazione e razionalizzazione del mondo applicativo tramite gli standard j2EE/.net, progettazione e sviluppo in ambiente Cloud, Social Platform, progettazione e sviluppo di servizi e contenuti Mobile (Android, iOS, Windows Mobile) e TV.

**ECM & Portal**

Per la gestione dei processi documentali e per un supporto completo alla dematerializzazione. Consoft Sistemi offre soluzioni di gestione documentale verticali facilmente integrabili ed è in grado di fornire sia competenze tecnologiche che normative. Nell'area dell'Enterprise Portal l'offerta propone soluzioni che sfruttano le migliori tecnologie oggi presenti sul mercato in grado di soddisfare requisiti di integrabilità, collaboratività, usabilità e sicurezza come Liferay, Alfresco e Microsoft SharePoint. La partnership strategica con Adobe System, leader nelle soluzioni ECM, completa l'offerta.

#### Extended Enterprise

Per aumentare la capacità dell'impresa di integrarsi con l'ambiente circostante fatto di Clienti, Fornitori, Partner, partendo dalla conoscenza dei processi aziendali maturata in anni di attività consulenziale attraverso la realizzazione di importanti progetti ERP. Consoft Sistemi Consulting è SAP Extended Business Member. I temi di integrazione principali riguardano il collegamento del SAP Business Warehouse con le soluzioni Business Objects, l'integrazione di Microsoft SharePoint tramite la soluzione Duet Enterprise e l'offerta di modulistica Adobe denominata Interactive Forms che facilita il colloquio con SAP.

#### Telecomunicazioni

Per supportare le aziende del settore TLC nella realizzazione di servizi innovativi a valore aggiunto, nella progettazione di reti (sia wireless che wired, con particolare attenzione alle nuove tecnologie quali le POF), nella gestione delle architetture di nuova generazione, nella realizzazione di applicazioni verticali, nella qualificazione di apparati e di piattaforme, nella progettazione di soluzioni in ambito digitale terrestre e satellitare. L'offerta in ambito TLC comprende inoltre la formazione tecnica nell'ambito delle reti di telefonia mobile, soluzioni di tele-assistenza, tele-monitoraggio, info-mobilità e localizzazione.

### 1.2.2 Descrizione dei capitoli

Individuato nel capitolo 1 il contesto principale che pone le basi per l'intera trattazione della tesi, il capitolo 2 affronta la formazione del sistema normativo europeo ed italiano (in particolar modo) in materia di firme elettroniche, dedicando, nello specifico, ampio spazio all'analisi delle loro diverse declinazioni (firme semplici, firme avanzate, firme qualificate, ecc.) e dei differenti effetti giuridici e risvolti legali che comporta il loro utilizzo.

Focalizzata l'attenzione sulla normativa che riguarda le firme elettroniche avanzate, il capitolo 3 propone una disamina dei principali campi di applicazione e delle tecnologie crittografiche di base che ne regolano il funzionamento; tema di particolare interesse è quello delle tecnologie biometriche applicate al processo di firma, che godono di una popolarità ed utilità in tutti quegli ambiti in cui l'apposizione di una firma è una pratica frequente; la biometrica di firma ha permesso la nascita di nuovi scenari applicativi (in primis quello della firma su tablet elettronico anziché su foglio di carta), senza richiedere un cambio di abitudini da parte dell'utente e mantenendo certi standard di sicurezza e privatezza dei dati.

Il capitolo 4 espone alcuni concetti di preparazione all'analisi progettuale, oggetto della seconda parte della tesi; offre una panoramica generale dei principali strumenti software adottati per la realizzazione di una applicazione client stand-alone in ambito desktop.

Il capitolo 5 è interamente rivolto alla progettazione della soluzione di firma elettronica avanzata: la discussione si concentra sull'analisi delle classi, delle funzioni e delle librerie utilizzate per gli scopi previsti, nonché sulla descrizione dei moduli, delle interfacce e delle strutture dati.

Sulla base di quanto esposto nel capitolo precedente, il capitolo 6 tratta invece del processo vero e proprio di firma, illustrando un tipico esempio di utilizzo dell'applicazione da parte di un utente firmatario.

Infine, il capitolo 7 (capitolo conclusivo), propone una serie di considerazioni finali sull'introduzione della biometria nelle nuove realtà applicative, che possono dare seguito a possibili sviluppi futuri della soluzione presentata.

# Capitolo 2

# Analisi normativa sulla firma elettronica

## 2.1 Abbreviazioni

La tabella seguente fornisce un elenco delle abbreviazioni normative e giuridiche adottate in questo capitolo e nel testo in generale:

| *abbreviazione* | *descrizione* |
|---|---|
| UE | Unione Europea |
| PE | Parlamento Europeo |
| CE | Comunità Europea |
| TU | Testo Unico |
| CAD | Codice dell'Amministrazione Digitale |
| PA | Pubblica Amministrazione |
| GU | Gazzetta Ufficiale |
| GUCE | Gazzetta Ufficiale della Comunità Europea |
| c.c. | Codice Civile |
| DLgs | Decreto Legislativo |
| DL | Decreto Legge |
| DPR | Decreto del Presidente della Repubblica |
| DPCM | Decreto del Presidente del Consiglio dei Ministri |

Tabella 2.1. Abbreviazioni giuridiche.

## 2.2 Formazione del sistema normativo italiano

L'Italia è stato il primo paese della UE a legiferare sul tema della firma digitale e a predisporre i relativi regolamenti. A breve seguì la Germania, quindi gli altri stati si mossero dopo la promulgazione della direttiva europea (vedi 2.3).

Dal punto di vista legislativo, l'atto formale che sancisce l'inizio della partecipazione dello stato italiano in materia di documentazione informatica e firma digitale va ricercato nella legge sulla "Riforma della pubblica amministrazione e per la semplificazione amministrativa, ossia la legge 15 marzo 1997, n. 59[1] (nota come Legge Bassanini). Tale legge conferisce:

[1] In GU n. 63 del 17 marzo 1997.

> Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa

Di matrice europea, sovranazionale, la legge Bassanini si configura come *legge delega*, finalizzata principalmente a dare al governo la capacità di sviluppare una profonda attività di innovazione e riforma del sistema amministrativo italiano. Dei 22 articoli di cui è composta, l'articolo 15 risulta di particolare rilevanza per il tema che verrà affrontato; il comma 2° recita:

> Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalità di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare entro centottanta giorni dalla data di entrata in vigore della presente legge [...]

Con il comma 2° viene sancito il pieno valore giuridico dei documenti informatici, i quali sono validi e rilevanti a tutti gli effetti di legge (2.4.1). Lo stesso anno, con il DPR 10 novembre 1997, n. 513[2], in osservanza di quanto disposto dall'articolo sopracitato, è stato emanato il:

> Regolamento recante i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2°, della legge 15 marzo 1997, n. 59

Con questo DPR la firma digitale entra ufficialmente a far parte del sistema giuridico italiano.

Il sistema legislativo italiano non solo si impegna in breve tempo a promulgare uno o più decreti volti a conferire autonomia alle regioni ed enti locali, per l'emanazione di specifici regolamenti che definiscano i domini applicativi delle norme descritte (il decreto prescrive, infatti, all'articolo 3, comma 1°, che siano fissate le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici), ma consente di stabilire in breve tempo le regole in base alle quali un ente (pubblico o privato) possa vedersi riconosciuto il ruolo di certificatore per la firma digitale[3] ed essere iscritto, su esplicita richiesta da parte dello stesso ente, nell'elenco pubblico dei certificatori, assegnando alla **AIPA**[4] il compito di supervisionare, approvare e mantenere aggiornato tale elenco. Il presidente della Repubblica, con il DPR 28 dicembre 2000, n. 445[5] emana il:

> Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa

che, tra l'altro, riprende le norme del DPR 10 novembre 1997, n. 513 sulla firma digitale, il quale pertanto viene abrogato.

Successive modifiche del TU saranno apportate, per quanto riguarda la firma elettronica (la cui normativa è di derivazione comunitaria, si veda la sezione 2.3), dal:

---

[2] In GU n. 60 del 13 marzo 1998.

[3] Figura inedita del nostro ordinamento che sarà in seguito riferita con l'accezione europea di "prestatore di servizi di certificazione", secondo l'articolo 2 della direttiva 1999/93/CE del Parlamento Europeo.

[4] Autorità per l'Informatica nella Pubblica Amministrazione, in seguito trasformata in **CNIPA** (Centro Nazionale per l'Informatica nella Pubblica Amministrazione), in attuazione di quanto disposto dal DLgs 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali". Il CNIPA è in seguito confluito in **DigitPA** (ente nazionale per la digitalizzazione della pubblica amministrazione), in attuazione di quanto disposto dal DLgs 1 dicembre 2009, n. 177. Con il DL 15 giugno 2012, n. 147 è stata istituita l'Agenzia per l'Italia digitale, che eredita la precedente gestione DigitPA e ha il compito di portare avanti gli obiettivi posti nell'Agenda Digitale Italiana (ADI).

[5] In GU n. 42 del 20 febbraio 2001.

- DLgs 23 gennaio 2002, n. 10[6] "Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche", che ha riconosciuto valore giuridico alla firma elettronica, oltre che alla firma digitale;
- DPR 7 aprile 2003, n. 137[7] "Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10".

Infine ulteriori modifiche saranno compiute a seguito dell'introduzione del **CAD**[8] con il DLgs 7 marzo 2005, n. 82, che abrogherà il DLgs 23 gennaio 2002, n. 10 e una serie di articoli del TU.

Gli obiettivi che il sistema normativo italiano intende conseguire sono chiari: apportare benefici e semplificazioni alla pubblica amministrazione e ai privati, assegnando valore giuridico alla firma digitale e ai documenti informatici sottoscritti digitalmente che in questo modo possono essere, ai sensi di legge, resi sostitutivi dei corrispondenti documenti cartacei. La firma digitale sarà quindi utilizzata non solo per la sottoscrizione di un documento informatico, ma sarà impiegata come strumento principale nel processo di fatturazione elettronica, nello scambio di documenti digitali in ambito amministrativo, nel processo di autenticazione dei firmatari.

## 2.3 Direttiva 1999/93/CE del Parlamento Europeo

Contestualmente all'emanazione della legge 15 marzo 1997, n. 59 (legge Bassanini), il PE ha dato ulteriore slancio al processo legislativo, ponendosi in prima linea nella stesura di un quadro di regole europee che garantiscano la libera circolazione dei prodotti dell'industria.

Di due anni posteriore, la direttiva europea[9] ignora del tutto l'esperienza italiana (nonostante fosse già consolidata su questa materia), ispirandosi a temi quali il commercio elettronico (e-commerce) e i concetti di liberalizzazione. Dell'impostazione nazionale non vengono ripresi i propositi di grande precisione normativa e tecnica (considerazioni tecniche vengono infatti ignorate nella direttiva, almeno nella sua prima stesura), né viene rafforzato lo spirito di concretezza che deriva dall'adottare un unico tipo di firma, quella digitale, caratterizzata da un elevato livello di sicurezza [2].

L'Europa guarda al mercato: l'idea che avanza è quella di concepire un sistema internazionale, valido giuridicamente, che indichi le condizioni sotto le quali è garantito il commercio elettronico tra i paesi membri; il dibattito vede contrapposte essenzialmente due visioni: una orientata a dotare l'intero sistema di un solido impianto normativo-giuridico, l'altra invece (di cui la direttiva è promotrice) che punta al libero commercio dei prodotti e alla libera iniziativa in un mercato aperto, a scapito dei controlli di sicurezza.

La visione italiana è dunque difforme da quella europea: ciò ha creato non pochi problemi di compatibilità in fase di recepimento della direttiva, il che ha portato a rilevanti modificazioni nell'impostazione delle norme italiane in vigore già da qualche anno. Modifiche imprescindibili poiché, come recita la stessa direttiva, vi è la necessità di adesione degli stessi Stati alle normative europee sul tema della firma elettronica, necessaria per l'autenticazione dei dati e l'**interoperabilità** dei prodotti elettronici ("considerando" n. 4 della direttiva):

> la divergenza delle norme in materia di riconoscimento giuridico delle firme elettroniche e di accreditamento dei prestatori di servizi di certificazione negli Stati Membri può costituire un grave ostacolo all'uso delle comunicazioni elettroniche e del commercio elettronico; invece, un quadro comunitario chiaro relativo alle condizioni che si

[6] In GU n. 39 del 15 febbraio 2002.

[7] In GU n. 138 del 17 giugno 2003, testo in vigore dal 2 luglio 2003.

[8] Codice dell'Amministrazione Digitale.

[9] In GUCE del 19 gennaio 2000.

> applicano alle firme elettroniche rafforzerà la fiducia nelle nuove tecnologie e la loro accettazione generale; la normativa negli Stati membri non dovrebbe essere di ostacolo alla libera circolazione di beni e di servizi nel mercato interno

Così chiosa Pierluigi Ridolfi nel suo libro [2]:

> I problemi che sta creando il recepimento della direttiva nel nostro sistema legislativo unitamente alla percezione che il suo valore aggiunto è inapprezzabile porta alla conclusione che di questa direttiva non si sentiva proprio il bisogno

La direttiva europea è stata recepita in Italia con il DLgs 23 gennaio 2002, n. 10, come viene precisato nella sezione precedente (2.2).

La figura 2.1 presenta in maniera organica e sintetica il processo di evoluzione temporale della normativa italiana, evidenziandone i singoli sviluppi prima e dopo l'ingresso della direttiva europea nel panorama internazionale:

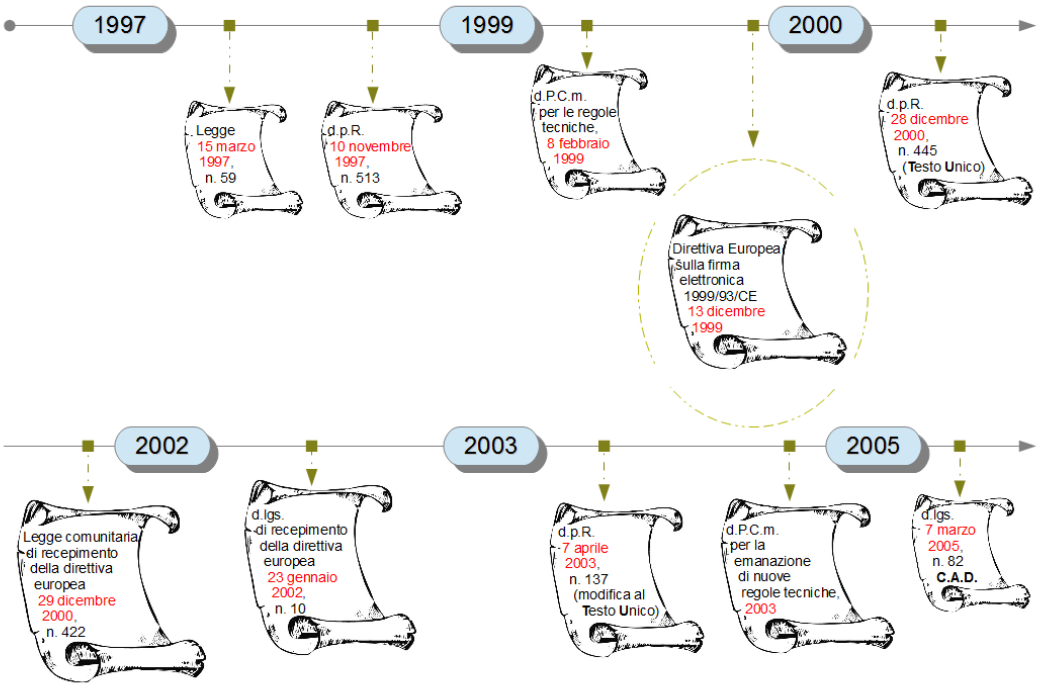


Figura 2.1. Evoluzione della normativa.

### 2.3.1 Definizioni europee: le origini delle firme elettroniche

Qui di seguito un elenco di definizioni ufficiali contenuti nella precedente direttiva europea (articolo 2):

- firma elettronica;
- firma elettronica avanzata;
- firmatario;

- dati per la creazione di una firma;
- dispositivo per la creazione di una firma;
- dispositivo sicuro per la creazione di una firma;
- dati per la verifica della firma;
- dispositivo di verifica della firma;
- certificato;
- certificato qualificato;
- prestatore di servizi di certificazione;
- prodotto di firma elettronica;
- accreditamento facoltativo.

Nella sezione 2.4 verranno illustrate le tipologie di firme attualmente vigenti nel sistema normativo e legislativo italiano.

### 2.3.2 Tipi di firme

La struttura normativa dettata dal legislatore comunitario determina una serie di differenti tipi di firme (o differenti livelli di sottoscrizione).

Occorre, per necessità di correttezza, notare che l'uso del termine "firma", in questo contesto, è del tutto improprio, tanto più che il contesto di cui parliamo è quello giuridico; sarebbe preferibile il termine "sottoscrizione". La differenza è sostanziale: la **firma** è definita come l'insieme dei simboli che costituisce il nome e cognome scritti, mediante autografia, su un documento; la **sottoscrizione** è invece il processo di apposizione di una firma alla conclusione di una lettera, un documento, o qualsiasi altra forma di scrittura, che assegna valore giuridico alla firma stessa [3]:

> La sottoscrizione conferisce la paternità al documento cartaceo, è il suggello della sua appartenenza a un soggetto: su di essa si è sviluppata la tradizione giuridica dal diritto romano sino ad oggi

Sebbene tutta la normativa sulla firma elettronica riguardi in effetti la sottoscrizione, in questo capitolo e nei successivi i due termini saranno utilizzati indifferentemente.

I differenti tipi di firme, in base alle caratteristiche di sicurezza offerte, possono ricadere nelle categorie principali di **firma elettronica** o di **firma elettronica avanzata**. Entrambe le categorie sono state recepite integralmente dal nostro sistema giuridico al quale, a seguito di successive modifiche del TU e del CAD, sono state aggiunte le categorie di **firma qualificata** e **firma digitale** (quest'ultima in particolare già presente a partire dal DPR 10 novembre 1997, n. 513).

## 2.4 Codice dell'Amministrazione Digitale

I tipi di firme che invece sono previste nel nostro sistema legislativo sono il risultato di una serie di introduzioni, modifiche ed integrazioni alle normative in materia di documentazione amministrativa che si sono succedute nel tempo; come già anticipato (sezione 2.2) la firma digitale viene istituita con il DPR 10 novembre 1997, n. 513, quindi ripresa nel TU.

Il testo cui oggi facciamo riferimento è il **Codice dell'Amministrazione Digitale (CAD)**, un "corpo organico di disposizioni" in materia informatica attraverso il quale continua il processo di rinnovamento della PA, posto in essere con il DLgs 7 marzo 2005, n. 82 ed entrato in vigore in

data 1 gennaio 2006; una serie di modifiche sono state apportate al CAD con il DLgs 4 aprile 2006, n. 159, che ha riordinato e consolidato la normativa vigente e con il DLgs 30 dicembre 2010, n. 235, che prevede l'emanazione di nuove regole tecniche in materia di firma digitale, firma elettronica qualificata e firma elettronica avanzata.

La figura 2.2 mostra la sequenza delle principali modifiche apportate al CAD, dalla sua costituzione fino ad oggi.

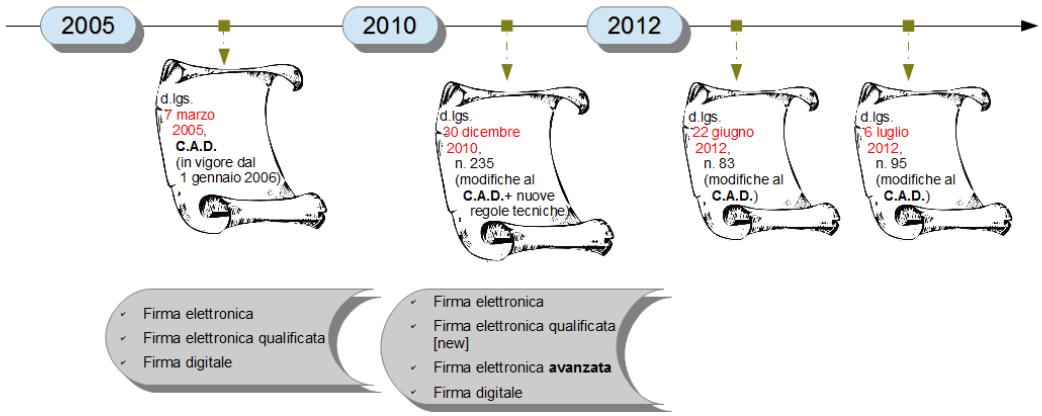


Figura 2.2. Principali modifiche al CAD.

Le firme previste sono attualmente quattro:

- firma elettronica;
- firma elettronica avanzata;
- firma elettronica qualificata;
- firma digitale.

In particolare le recenti modificazioni al codice hanno portato all'introduzione della firma elettronica avanzata.

Prima di procedere con l'analisi delle firme informatiche ad oggi a nostra disposizione, è utile soffermarsi brevemente sul processo di innovazione che ha riguardato il concetto di documento informatico, la cui definizione è stata ed è ancora oggi oggetto del dibattito giuridico in materia di amministrazione digitale.

### 2.4.1 Il documento informatico

Risultato finale del processo di dematerializzazione di cui si è fatto riferimento nel capitolo 1, nonché elemento essenziale su cui si fonda l'intera struttura concettuale delle firme informatiche,

il **documento informatico** è definito nel CAD (DLgs 7 marzo 2005, n. 82, articolo 1, comma 1° e successive modifiche) come:

> la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti

Si tratta certamente di una definizione di ampio respiro, in cui ricadono forme di vario genere: un video digitale o un file di testo, così come un messaggio di posta elettronica sono esempi di documento informatico.

Il tema che il legislatore italiano ha dovuto affrontare nel tempo (e la cui soluzione finale risultante da vari interventi è confluita nell'ultima versione del codice) è la formazione di una normativa del documento che tenesse in considerazione il passaggio dal sistema tradizionale in uso (documento cartaceo) ad un sistema di natura informatica, digitalizzata, e che dotasse il documento di una efficacia in sede probatoria: il codice vigente centra l'obiettivo di parificare, in termini legali, il documento informatico al documento in forma scritta; il legislatore realizza quindi una soluzione di continuità, superando però non pochi problemi.

Innanzitutto con il documento informatico viene a mancare il legame (inscindibile nel documento cartaceo) tra informazione (o contenuto) e il supporto relativo: se in un contesto tradizionale era sempre possibile fare una distinzione tra documento originale e copia, nell'era digitale è possibile trasferire il documento da un supporto ad un altro, trasmetterlo a distanza, farne una copia, ecc., mantenendo inalterata la sequenza dei bit; il contenuto è svincolato dal suo supporto. Viene a mancare quindi il requisito di materialità che ha finora contraddistinto il documento tradizionale, portando ad affermare l'immaterialità del documento informatico, con la conseguenza che [4]:

> in nessun punto della normativa sul documento informatico il supporto è determinante per la natura del documento informatico. Esso esiste indipendentemente dal supporto, è una realtà immateriale, cioè l'esatto opposto della *res signata* della dottrina tradizionale

Per dotare il documento informatico di una predeterminata efficacia, il legislatore ha anche dovuto affiancare all'originaria definizione una serie di disposizioni che imponessero l'uso delle firme elettroniche da apporre ai documenti (articolo 21, comma 1°):

> Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, integrità e immodificabilità

Ma il passo che disciplina il **requisito di forma scritta al documento informatico** lo si ritrova nell'articolo 20, comma 2°:

> Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche [...] ha l'efficacia prevista dall'articolo 2702 del codice civile [...]

Il legislatore, dunque, attribuisce piena efficacia legale solo ai documenti sottoscritti con firma elettronica avanzata, qualificata o firma digitale (la quale garantisce, nei documenti informatici, gli stessi requisiti garantiti dalla firma autografa nei documenti cartacei), lasciando che il valore probatorio, e quindi il requisito di forma scritta, di un documento sottoscritto con firma elettronica "semplice" sia liberamente valutabile in giudizio in base a caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità (articolo 20, comma 1-bis).

Sarà, in conclusione, compito del giudice esprimere di volta in volta un giudizio sul valore probatorio di un documento sottoscritto con una firma elettronica semplice.

### 2.4.2 Firma elettronica

Definizione (trattasi di quella recepita dalla direttiva, in seguito però modificata):

> un insieme di dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione

Quello di firma elettronica è un concetto di carattere generale, introdotto nel nostro sistema normativo per effetto della direttiva europea (DLgs 23 gennaio 2002, n. 10) e rimasto quasi del tutto immutato nelle modifiche successive al CAD.

La genericità e la mancanza di espliciti riferimenti a soluzioni tecnologiche lasciano spazio a varie interpretazioni della definizione [5]: innanzitutto l'espressione *insieme di dati in forma elettronica* non fa luce sulla reale natura della firma: basandosi su quanto scritto, anche la scrittura del nome e cognome in calce ad una email od a un documento informatico costituisce una firma elettronica, così come la semplice immagine di una firma autografa allegata ad un documento digitale (in luogo della firma autografa stessa) di fatto rappresenta una firma elettronica; anche l'espressione *associazione logica* non rende noto con precisione il tipo di legame che intercorre tra il documento di cui la firma vuole essere la sottoscrizione e la firma stessa: una firma, in tal caso, non deve essere necessariamente apposta al documento da firmare per essere una firma elettronica, se viene stabilito un qualche legame tra il documento originale e quello su cui è effettivamente presente la firma. Richiede un'ulteriore attenzione l'espressione *metodo di autenticazione*: questa infatti deriva da un'errata (o comunque non corrispondente a quanto inteso nella direttiva europea) dall'inglese "method of authentication", a cui si sarebbe forse preferita la locuzione "metodo di autenticità". La nozione di autenticazione è regolamentata dall'articolo 2703, comma 2°, del codice civile:

> l'autenticazione consiste nell'attestazione da parte del pubblico ufficiale che la sottoscrizione è stata apposta in sua presenza. Il pubblico ufficiale deve previamente accertare l'identità della persona che sottoscrive

Per le motivazioni di cui sopra, l'entrata in vigore del codice ha dato l'occasione per modificare la definizione di firma elettronica in precedenza recepita integralmente nella sua versione originale; la variazione più importante riguarda per l'appunto la sostituzione del termine "autenticazione" con quello di "identificazione informatica", il che rende ragione a quanto argomentato prima. Ecco la definizione attualmente vigente:

> l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica

Il decreto non indica le caratteristiche tecniche né il livello di sicurezza previsto dalla firma elettronica (essa può essere una password, una firma autografa digitalizzata mediante scanner, una firma biometrica), non prevede meccanismi di autenticazione del firmatario o di integrità dell'insieme dei dati firmati, di conseguenza questa è da ritenersi la forma più debole di firma in ambito informatico.

Concludendo, la firma elettronica semplice può essere adottata per dotare il documento informatico di una certa efficacia legale e il suo valore probatorio sarà liberamente valutabile in giudizio in base a caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità (vedi 2.4.1).

### 2.4.3 Firma elettronica qualificata

È definita come:

> la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare

> un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi sono stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma

Si tratta di una forma sicura di firma, introdotta nel CAD alla sua prima stesura, la cui definizione risponde alle esigenze in precedenza espresse dalla direttiva europea[10], grazie all'aggiunta dell'utilizzo di un certificato qualificato[11] (tramite cui possa avvenire l'associazione del firmatario con il documento firmato) e di un dispositivo sicuro di firma.

La firma elettronica qualificata corrisponde alla "Qualified electronic signature" definita da ETSI[12]. L'ordinamento giuridico prevede di riservare alla sola firma elettronica qualificata la possibilità di sottoscrizione dei seguenti atti (articolo 2643 c.c.):

> contratti che, in relazione a beni immobili, ne trasferiscano la proprietà, costituiscano, modifichino o trasferiscano l'usufrutto, il diritto di superficie, il diritto del concedente o dell'enfiteuta, la comunione su tali diritti, le servitù prediali, il diritto di uso, il diritto di abitazione, atti di rinuncia dei diritti precedenti, contratti di affrancazione del fondo enfiteutico, contratti di anticresi, contratti di locazione per una durata superiore a nove anni; contratti di società o di assicurazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo determinato; gli atti che costituiscono rendite perpetue o vitalizie, salve le disposizioni relative alle rendite di Stato; gli atti di divisione di beni immobili e di altri diritti reali immobiliari; le transazioni che hanno per oggetto controversie relative ai diritti di cui sopra

### 2.4.4 Firma elettronica avanzata

Ecco la definizione:

> la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati

In un primo momento eliminata con l'entrata in vigore del codice ed in seguito reintrodotta con il DLgs 30 dicembre 2010, n. 235, la definizione di firma elettronica avanzata[13] riprende esattamente quella originale presente nella direttiva europea, di seguito riportata nella sua forma integrale (articolo 2 della direttiva):

> "firma elettronica avanzata", una firma elettronica che soddisfi i seguenti requisiti:
>
> - essere connessa in maniera unica al firmatario[14];
> - essere idonea ad identificare il firmatario;

[10] Gli effetti giuridici previsti dalla direttiva si riferiscono infatti a "firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura", cioè alle "firme qualificate".

[11] Il certificato non è menzionato, invece, nella definizione di firma elettronica avanzata.

[12] European Telecommunications Standards Institute.

[13] Nei successivi capitoli indicata con la sigla FEA.

[14] Come sia associata la firma elettronica avanzata al firmatario, la definizione non lo precisa.

- essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;
- essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

Sulla scorta della bozza sulle regole tecniche[15] (che dovrebbero a breve essere approvate in via definitiva), possiamo desumere una serie di profili: le firme elettroniche avanzate non fanno riferimento a nessun tipo di tecnologia predefinita, né ad un particolare software di creazione firma (gli sviluppatori di soluzioni di firme elettroniche avanzate hanno quindi assoluta libertà applicativa e tecnologica); non vi è l'obbligo di un controllo preventivo da parte degli organi preposti alla vigilanza (gli enti che forniscono servizi di questo tipo non sono vincolati alla registrazione presso di essi); la normativa lascia quindi ampia libertà di azione ai soggetti che realizzano per proprio conto soluzioni di firma elettronica avanzata, sebbene debbano adempiere ad una serie di obblighi, tra cui la necessità di (articolo 57, comma 1°):

> identificare in modo certo l'utente (tramite un valido documento di riconoscimento) e informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente

In pieno spirito di liberalizzazione delle tecniche di firma voluta dalla direttiva europea (essa si basa infatti sul principio del *technology-neutral*), le firme elettroniche avanzate vogliono rappresentare quindi uno strumento neutro, facilmente adattabile al contesto in cui si realizza tale firma, ma orientato a mantenere la sicurezza delle informazioni coinvolte nel processo: devono infatti essere garantite anche l'integrità e la leggibilità dei dati firmati.

Ai sensi dell'articolo 61 della bozza sopracitata, l'invio tramite posta elettronica certificata costituisce, nei confronti della pubblica amministrazione, firma elettronica avanzata. Anche la Carta d'Identità Elettronica o la Carta Nazionale dei Servizi sono utilizzabili dalle pubbliche amministrazioni per realizzare sistemi di firma elettronica avanzata. Può trattarsi di firma elettronica avanzata una OTP[16], la stessa firma biometrica o la firma generata tramite un tablet, purché se ne verifichino le caratteristiche e si garantisca la riconducibilità del documento informatico (non modificato) al soggetto firmatario.

Rappresenta una forma più forte rispetto alla firma elettronica per l'introduzione delle sopracitate caratteristiche di sicurezza, sebbene il suo dominio di applicazione sia limitato, se confrontato con quello previsto per la firma elettronica qualificata o la firma digitale (ricordiamo infatti che, a differenza di queste ultime, la firma elettronica avanzata non è vincolata all'utilizzo di un certificato qualificato o ad un dispositivo sicuro di creazione della firma); essa non sarà sufficiente, ad esempio, per la firma di atti aventi ad oggetto beni immobili (articolo 1350 c.c.), ma possono essere sottoscritti (con firma elettronica avanzata o elettronica) unicamente, oltre agli atti non formali, solo gli altri atti indicati dalla legge per cui sia prevista la forma scritta *ad substantiam* (articolo 1350 c.c.); tra questi ci sono i contratti bancari e di intermediazione mobiliare. L'articolo 60 tratta dei limiti d'uso della firma elettronica avanzata:

> La firma elettronica avanzata realizzata in conformità con le disposizioni delle presenti regole tecniche, è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto di cui all'art. 55, comma 2°, lettera a[17].

[15] Bozza DPCM 06 luglio 2011: "Regole tecniche in materia di generazione, apposizione, e verifica delle firme elettroniche avanzate, firme elettroniche qualificate, firme elettroniche digitali e validazione temporale dei documenti informatici".

[16] One Time Password.

[17] Ossia i soggetti che erogano i servizi per proprio conto e non per la fornitura a terzi, quale scopo dell'attività d'impresa.

**Novità recenti**

Nel mese di dicembre 2012 vi sono stati importanti sviluppi sul piano legislativo che regolamentano ulteriormente le firme elettroniche avanzate.

Il DL 18 ottobre 2012, n. 179, convertito nella legge 17 dicembre 2012, n.221 introduce alcuni emendamenti all'attuale normativa del CAD, in particolare stabilisce che il disconoscimento di un documento informatico sottoscritto con firma elettronica avanzata non è basato sulla prova del mancato utilizzo del dispositivo di firma (in quanto essa non si basa necessariamente su un dispositivo di firma), sebbene tale disconoscimento riguardi ancora le firme qualificate e digitali (modifica all'articolo 21, comma 2° del CAD): le forme di disconoscimento dovranno quindi essere individuate caso per caso.

### 2.4.5 Firma elettronica qualificata (modificata)

Il DLgs 30 dicembre 2010, n. 235 propone una nuova versione della definizione di firma elettronica qualificata, in seguito all'introduzione della firma elettronica avanzata:

> firma elettronica avanzata basata su un certificato qualificato e generata mediante un dispositivo sicuro di creazione della firma

### 2.4.6 Firma digitale

Definizione:

> un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici

Il legislatore italiano riprende la definizione di firma digitale introdotta nell'originaria normativa nazionale (DPR 10 novembre 1997, n. 513) arricchendola a fronte delle recenti modifiche al CAD: si tratta di una firma elettronica qualificata, quindi di una firma elettronica avanzata basata su un certificato qualificato, generata mediante un dispositivo sicuro di creazione della firma, che adotta un sistema di chiavi asimmetriche.

Un certificato che non sia qualificato non è sufficiente per disporre dei requisiti del livello più elevato di qualità e sicurezza; occorre che il certificatore che emette il certificato sia accreditato presso il DigitPA (ente istituzionale che svolge attività di vigilanza sui certificatori, adesso confluito nell'Agenzia per l'Italia digitale, come indicato in precedenza) e quindi regolarmente iscritto nell'apposito elenco pubblico dei certificatori accreditati (per un approfondimento sul tema dei certificati si veda la sezione 3.2.4 del capitolo 3). La firma digitale accompagnata da un certificato rilasciato da un certificatore accreditato è il tipo di firma richiesta per sottoscrivere (articolo 38 del TU):

> tutte le istanze e le dichiarazioni da presentare all'amministrazione o ai gestori o esercenti di pubblici servizi

Ad essa corrisponde il massimo livello di sicurezza informatica ed è equivalente ad una sottoscrizione autografa (assolve al requisito giuridico della forma scritta).

### 2.4.7 Differenze tra le firme e conclusioni

La differenza principale tra i tipi di firma riguarda sicuramente la tecnologia adottata: se le definizioni di firma elettronica e di firma elettronica avanzata non fanno riferimento ad una tecnologia in particolare, quelle di firma elettronica qualificata e digitale sono associate ad una tecnologia ben definita, così come a livelli di sicurezza predeterminati [6].

La presenza di molteplici firme nel panorama legislativo ha portato ad adottare, nel linguaggio corrente, le espressioni di "firme leggere" (o firme deboli) e "firme forti". La normativa sancisce che l'unico tipo di firma che ricade nella seconda categoria sia la firma digitale, in base alle caratteristiche di sicurezza intrinseche offerte; firma elettronica, firma elettronica avanzata e in generale tutto ciò che non risponde alla definizione data per la firma digitale fa parte dell'insieme delle firme leggere. Si vedano in particolare le figure 2.3 e 2.4.

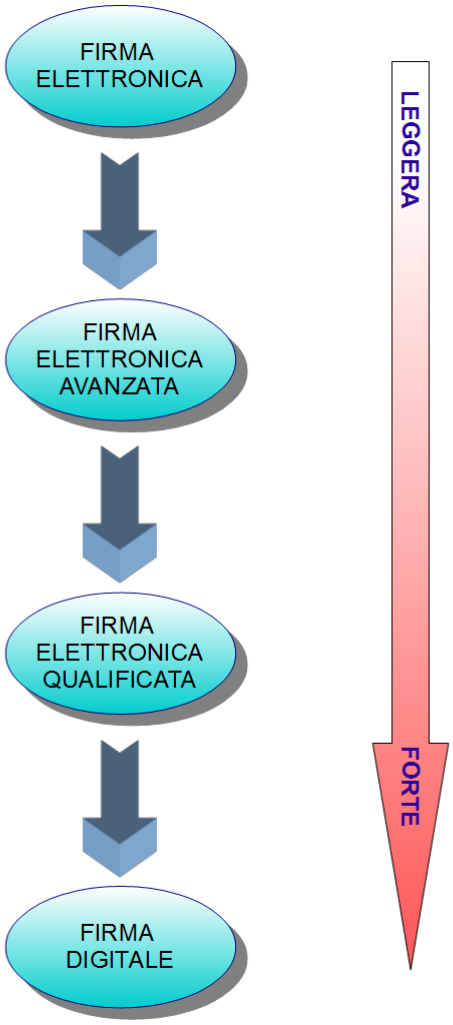


Figura 2.3. Firme leggere, firme forti.

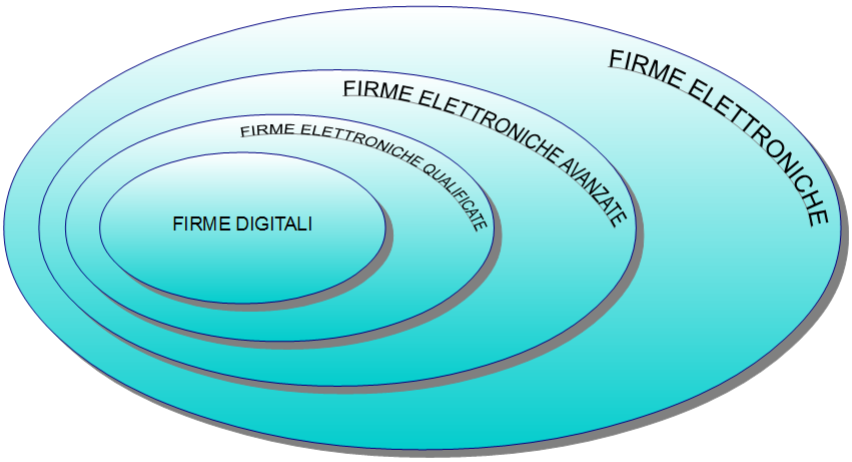


Figura 2.4. Differenti tipi di firme.

# Capitolo 3

# FEA: applicazioni pratiche

Come già anticipato nel capitolo 1, il passaggio da forme di documentazione cartacee ai già citati documenti informatici è ancora oggi in fase di completamento, sebbene il processo sia stato avviato già intorno alla metà degli anni '90; le recenti modificazioni ed adattamenti della legislazione italiana sul tema delle firme elettroniche (vedi capitolo 2), nonché la molteplicità di soluzioni tecnologiche a nostra disposizione hanno dato ulteriore impulso alla procedura di conversione, ponendo anzi le basi per la nascita di un nuovo processo, finalizzato alla creazione di documenti informatici "nativi", ossia svincolati del tutto dal supporto di carta.

## 3.1 Conservazione sostitutiva

L'atto di creazione di un documento informatico a partire dal suo equivalente analogico non può certo ridursi alla semplice scansione del documento stesso e la sua memorizzazione su un supporto informatico: è necessario infatti seguire un preciso trattamento tecnico-giuridico per garantire l'immutabilità di alcune caratteristiche del documento nella sua conversione al mondo digitale (si pensi, ad esempio, alla possibilità di verificarne l'autenticità o l'integrità).

La normativa italiana regolamenta le attività di digitalizzazione dei documenti in base ad una procedura, nota come **conservazione sostitutiva**. Questa è per l'appunto un metodo legale e informatico che determina le modalità in base alle quali compiere la sostituzione di documenti cartacei (che, a processo completo, consentirà di ridurre gli archivi cartacei, fino alla loro definitiva eliminazione) con gli equivalenti documenti in forma digitale i quali, sotto opportune condizioni, hanno piena validità legale (garantita nel tempo).

In figura 3.1 uno schema semplificato del processo di conservazione sostitutiva.

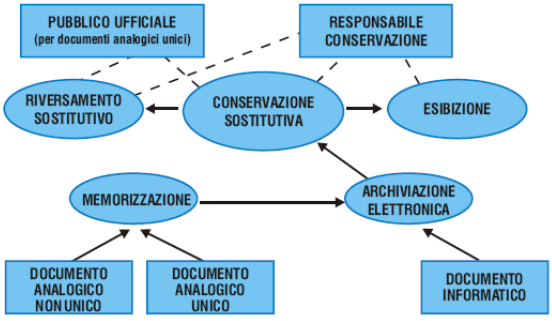


Figura 3.1. Processo di conservazione sostitutiva (fonte: Sispi).

Come sancito dalla Legge Bassanini (sezione 2.2) e più avanti dalla delibera del CNIPA del 19 febbraio 2004[1], l'unico tipo di firma elettronica avanzata adottata in questo contesto è specificamente la **firma digitale**, apposta al documento da parte del responsabile della conservazione, la cui tecnologia garantisce in modo univoco la paternità del documento firmato e la sua non modificabilità; dobbiamo infatti considerare che nel processo di dematerializzazione restano in sospeso alcuni problemi legati alla verifica dell'autenticità della firma autografa apposta al documento cartaceo; la firma digitale, in questo senso, se apposta al corrispondente documento digitalizzato, consente di dimostrare in sede legale l'appartenenza della firma al firmatario, nonché una precisa datazione del documento se affiancata da una cosiddetta marca temporale; gli articoli 3 e 4 esprimono con chiarezza quanto spiegato (distinguendo due diversi approcci secondo il tipo di documento da conservare).
Articolo 3 (conservazione sostitutiva di documenti informatici), comma 1°:

> Il processo di conservazione sostitutiva di documenti informatici, anche sottoscritti, [...], e, eventualmente, anche delle loro impronte [...] termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo

Articolo 4 (conservazione sostitutiva di documenti analogici), comma 1°:

> Il processo di conservazione sostitutiva di documenti analogici avviene mediante memorizzazione della relativa immagine direttamente sui supporti ottici, eventualmente, anche della relativa impronta, e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo

I benefici di questo processo sono numerosi:

- è possibile archiviare digitalmente grandi quantità di documenti cartacei su supporti di ridotte dimensioni, ottenendo una notevole riduzione di spazio occupato per conservare tali documenti (riduzione di costi e salvaguardia dell'ambiente);
- elevate capacità di ricerca e riproduzione dei documenti;
- possibilità di trasferimento in tempi ridotti (e con maggior semplicità) di elevate quantità di informazioni tra due parti fisicamente distanti tra loro;
- l'operazione di duplicazione dei documenti digitali non comporta perdita di qualità (si pensi invece al caso in cui si effettuino fotocopie a partire da altre fotocopie di documenti analogici, in cui è evidente la progressiva perdita di definizione dei caratteri stampati).

Come già anticipato nella sezione 1.1, i fattori di ostacolo alla realizzazione del processo di conservazione sostitutiva su larga scala (amministrazioni, enti istituzionali o privati, ecc.) sono comunque ancora presenti, anche se non di natura tecnica [7]: è di particolare rilevanza la nostra impreparazione culturale a svincolarci del tutto dal supporto tradizionale (la carta, per l'appunto), a favore di prodotti e tecnologie informatiche che contribuiscono all'innovazione e alla semplificazione delle operazioni più comuni; la scarsa conoscenza giuridica inoltre porta a pensare che i documenti digitalizzati a partire da quelli analogici non godano delle stesse caratteristiche ai sensi di legge; le norme tecnico-giuridiche esposte in precedenza contrastano con quest'ultimo punto, dato che garantiscono l'equivalenza legale (sotto certe condizioni) tra documento analogico e digitale.

[1] Deliberazione CNIPA n.11 del 19 febbraio 2004 "Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali.

La sezione seguente spiega il funzionamento generale della firma digitale (di cui è stato trattato l'aspetto normativo nella sezione 2.4.6) ed esamina le tecnologie previste dalla normativa nel processo di apposizione e verifica di una firma. I concetti esaminati nelle due sezioni successive saranno quindi ripresi nel capitolo 5.

## 3.2 Firma digitale

La firma digitale è un metodo informatico che genera un legame univoco tra l'autore (cui faremo in seguito riferimento con il termine *firmatario*) di un documento digitale e il documento stesso, garantendo una serie di proprietà di sicurezza; con una firma digitale è possibile infatti:

- impedire al firmatario di disconoscere il documento firmato (proprietà di **non ripudio**);
- permettere al destinatario (o ai destinatari, indicati altrimenti con il termine *verificatori*) del documento di verificare l'autenticità della firma (proprietà di **autenticità**);
- impedire la manipolazione o la modifica del documento (ad opera di utenti malintenzionati) senza invalidarne anche la firma (proprietà di **integrità**).

Il processo di apposizione di una firma ad un documento e della sua verifica si basa essenzialmente su due tecniche di sicurezza:

- Crittografia a chiave pubblica (asimmetrica);
- Funzioni di hash crittografiche.

### 3.2.1 Crittografia a chiave pubblica

La crittografia asimmetrica è una tecnica che consiste nella generazione di una coppia di chiavi, una pubblica e una privata, adottate per lo scambio di messaggi cifrati (dei quali si vuole garantire la proprietà di riservatezza, o privatezza) tra due entità; una chiave sarà utilizzata per la cifratura del messaggio, l'altra servirà invece per l'operazione di decifrazione e quindi di estrazione del messaggio originale (le chiavi hanno funzionalità reciproche, per questo motivo si parla in genere di chiavi asimmetriche, o simmetriche a coppie).

Questa nuova tecnica, sviluppata verso la metà del secolo scorso, supera certe limitazioni tipiche della cifratura simmetrica, legate all'utilizzo di una sola chiave (segreta) che pertanto doveva essere posseduta esclusivamente da parti reciprocamente fidate, "trusted", che intendevano comunicare con la garanzia che i dati scambiati non fossero resi noti ad entità terze.

Con la crittografia asimmetrica la strategia adottata è invece quella di dotare la coppia di chiavi di funzionalità certamente interscambiabili (se con una chiave si cifra, con l'altra si decifra e viceversa), ma allo stesso tempo le chiavi sono tra loro del tutto indipendenti, ossia non si è in grado di risalire ad una chiave conoscendo l'altra.

#### Contesti di generazione delle chiavi

Possiamo sostanzialmente individuare tre ambiti in cui si possa realizzare la generazione delle chiavi [8]:

1. il primo è quello in cui l'utente genera entrambe le chiavi mediante apposito software, dal proprio computer; la chiave privata viene quindi memorizzata sul disco rigido, in una posizione non accessibile a terzi, mentre la chiave pubblica è distribuita pubblicamente. Questa modalità espone a rischi per la sicurezza, in quanto il supporto di memorizzazione non è

idoneo a garantire la proprietà di riservatezza della chiave privata; si tratta quindi di una soluzione da limitare solo allo scambio di documenti digitali per i quali la segretezza non sia un requisito particolarmente importante; l'altro svantaggio è che gli interlocutori devono adottare lo stesso software di generazione chiavi;

2. il secondo ambito prevede che la generazione delle chiavi sia delegata ad enti specializzati che hanno la funzione di certificatori (si veda la sezione 3.2.4); il certificatore rilascia quindi la chiave privata all'utente, dando a questi anche la responsabilità di custodirla segretamente;

3. l'ultima opzione (e anche la più attuata) prevede che la generazione e la conservazione delle chiavi sia a carico di un *dispositivo di firma* (già più volte citato nel capitolo 2).

Una volta generata la coppia di chiavi, la **chiave pubblica** ($K_{pub}$) va comunicata a tutti i possibili interlocutori, la **chiave privata** ($K_{pri}$) è tenuta in segreto dall'utente che ne ha la proprietà. Gli algoritmi di cifratura e decifrazione devono invece essere pubblici.

Ma quali sono gli algoritmi di cifratura asimmetrica a nostra disposizione oggi nell'ambito delle firme digitali? La sezione seguente descriverà uno degli algoritmi più usati per la cifratura di firme[2], nonché quello che verrà più volte ripreso e considerato nelle soluzioni applicative dei capitoli seguenti.

### RSA

L'algoritmo di cifratura RSA (dalle iniziali dei nomi dei ricercatori americani del MIT[3] che lo hanno inventato, Ron Rivest, Adi Shamir, Leonard Adleman) si basa principalmente su alcune proprietà e applicazioni della teoria dei numeri primi e sull'aritmetica modulare.

Occorre premettere come tale algoritmo non sia sicuro dal punto di vista matematico-teorico, in quanto vi è la possibilità di risalire al messaggio in chiaro a partire dalla chiave pubblica; ma la grande quantità di calcoli e di tempo computazionale necessari per forzarlo lo rendono all'atto pratico un metodo tecnicamente invulnerabile, dotato di caratteristiche di sicurezza e di affidabilità totali.

Esso permette di fare riservatezza senza segreti condivisi e di generare firme digitali, nonché di garantire la provenienza del messaggio cifrato. Il procedimento matematico per la creazione delle due chiavi è il seguente:

1. vengono generati casualmente due numeri $P$ e $Q$ primi, grandi (elevato numero di cifre, necessario per garantire la sicurezza dell'algoritmo) e segreti. Indichiamo con $N$ il *modulo pubblico*, ottenuto dalla moltiplicazione di $P$ e $Q$: $N = P * Q$;

2. viene generato un numero $E$ (*esponente pubblico*), anch'esso in modo casuale, purché coprìmo (non ha nessun divisore in comune) e più piccolo di $(P-1)*(Q-1)$;

3. si calcola quindi un numero $D$ (*esponente privato*), tale che: $D = E^{-1}\ mod\ (P-1)*(Q-1)$;

4. posto che il valore del plaintext (ossia il messaggio in chiaro) $m$ sia minore di $N$, ossia $m < N$:

   - **chiave pubblica**: $K_{pub} = (N, E)$;
   - **chiave privata**: $K_{pri} = (N, D)$;
   - messaggio cifrato: $c = m^E\ mod\ N$;

[2] La Deliberazione CNIPA n. 45 del 21 maggio 2009 designa l'RSA come algoritmo principale di crittografia asimmetrica per la generazione e verifica della firma digitale, sebbene precisi che, a partire dall'anno successivo all'entrata in vigore di tale delibera, anche le firme elettroniche apposte utilizzando algoritmi di crittografia asimmetrica basati sulle curve ellittiche hanno lo stesso valore legale delle firme digitali.

[3] Massachusetts Institute of Technology.

- messaggio decifrato: $m = c^D \ mod \ N$.

Occorre adesso considerare alcuni aspetti.

Sebbene sia noto il modulo $N$, non lo sono i suoi fattori primi $P$ e $Q$, e non esiste alcun metodo matematico diretto (se non quello per tentativi) per risalire ad essi in tempi ragionevoli; in altri termini, non esiste una formula che consenta di verificare la *primalità* di un numero (verificare cioè se quel numero è primo), né di determinare la sua scomposizione in numeri primi; l'approccio per tentativi richiederebbe di eseguire una successione di divisioni del numero per tutti i numeri primi minori della sua radice quadrata: per valori elevati di $N$ ciò richiederebbe un tempo (e uno spazio di memoria) tale da non rendere fattibile l'operazione; l'efficacia dell'algoritmo RSA si basa proprio sull'elevata complessità del calcolo richiesto dalla fattorizzazione in numeri primi (problema NP-completo) [9].

Sia la chiave pubblica che la chiave privata sono generati a partire dal modulo $N$ il quale, in base a quanto esposto in precedenza, è funzione dei numeri primi $P$ e $Q$: la sicurezza dell'algoritmo dipenderà quindi strettamente dal modo in cui sono stati scelti tali numeri. Secondo quanto disposto dall'articolo 3 della Deliberazione CNIPA n. 45 del 21 maggio 2009, i certificatori accreditati devono utilizzare chiavi di lunghezza non inferiore a 1024 bit.

Si è già accennato in precedenza ad alcune caratteristiche salienti dell'algoritmo RSA: la garanzia di riservatezza e la verifica di provenienza del messaggio scambiato; in realtà lo stesso metodo consente anche di garantire l'integrità del messaggio: a patto che il destinatario conosca in anticipo il contenuto del messaggio ricevuto, questo è in grado di determinare, a seguito della decifrazione, se il messaggio non sia stato manipolato, semplicemente verificandone la coerenza con quanto atteso; sorge tuttavia un problema: l'algoritmo RSA (e in generale gli algoritmi asimmetrici) si prestano bene alla cifratura/decifrazione di messaggi corti, in genere un centinaio di bit; poiché in genere i messaggi hanno una dimensione maggiore (così come i documenti digitali che tratteremo nel prosieguo), tali operazioni risulterebbero particolarmente onerose dal punto di vista computazionale; sono state adottate delle soluzioni che garantiscono comunque l'integrità dei messaggi indipendentemente dalla loro lunghezza, consentendo di mantenere le caratteristiche di sicurezza sopracitate.

Una soluzione comune è quella di non applicare il meccanismo di cifratura all'intero messaggio, bensì ad un suo "riassunto" (detto impronta, o *digest*); l'algoritmo sarà dunque eseguito su una quantità di bit estremamente inferiore rispetto a quella del messaggio originale, il che riduce i tempi di realizzazione delle operazioni. La sezione seguente tratterà la seconda tecnica di sicurezza adottata nel contesto delle firme digitali, volta alla generazione di suddette impronte.

### 3.2.2 Funzioni di hash crittografiche

A partire da questa sottosezione si useranno scambievolmente i termini **impronta** e **message digest** per indicare un riassunto a lunghezza fissa del messaggio da proteggere, ottenuto mediante una funzione di hash crittografica. La definizione data dal DPCM sulle regole tecniche[4] per l'impronta è la seguente (vedi figura 3.2):

> impronta di una sequenza di simboli binari (bit): la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash

Per quanto riguarda la funzione di hash, la definizione è la seguente:

[4] Bozza DPCM 06 luglio 2011 sulle "Regole tecniche in materia di formazione, trasmissione, conservazione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni e di gestione del fascicolo informatico".

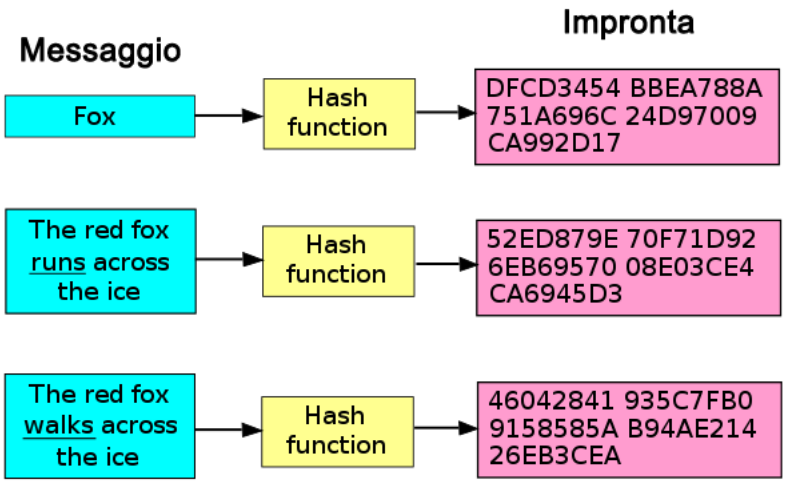


Figura 3.2. Message digest (fonte: Wikipedia, funzione crittografica di hash).

> una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti

Una funzione di hash $H$ applica quindi una trasformazione matematica ad un input $m$ e restituisce una stringa di simboli di dimensione fissa, chiamato valore di hash (o più semplicemente hash) $h$. In formule: $h = H(m)$. I requisiti base per una funzione di hash crittografica sono i seguenti:

- il dato in input può essere di lunghezza arbitraria;
- l'output (il digest) ha una lunghezza fissa;
- $H$ deve essere difficile da invertire: dato un valore di hash $h$, deve essere computazionalmente impossibile individuare un input $x$ tale che $H(x) = h$;
- la funzione di hash $H$ deve essere *collision-free*; occorre fare due distinzioni [10]:
  - se, dato un messaggio $x$, è computazionalmente impossibile trovare un messaggio $y$ diverso da $x$ tale che $H(x) = H(y)$, allora la funzione è detta *weakly collision-free*;
  - la funzione di hash è invece detta *strongly collision-free* se per essa è computazionalmente impossibile trovare due messaggi qualunque $x$ e $y$ tali che $H(x) = H(y)$.

La tabella 3.1 mostra un elenco dei principali algoritmi di hash crittografici, per ciascuno dei quali viene indicato il nome, la dimensione del blocco dati su cui opera, la dimensione del digest creato, la documentazione di riferimento. Evidenziato in rosso è l'algoritmo che, in base alla Deliberazione CNIPA n. 45 del 21 maggio 2009 (articolo 4), i certificatori accreditati devono utilizzare per la sottoscrizione di certificati elettronici di certificazione, di sottoscrizione e di marcatura temporale, nonché per la sottoscrizione delle relative CRL (analizzeremo più avanti il concetto di certificato relativo ad una firma digitale); tale algoritmo dovrà essere utilizzato anche per le applicazioni di generazione e verifica della firma digitale.

### 3.2.3 Processo di firma e verifica

Analizzate le tecniche di sicurezza su cui si basa la firma digitale, descriviamo il processo di creazione di una firma da parte di un firmatario e la sua verifica (svolta da un soggetto verificatore). Prenderemo a riferimento la figura 3.3.

| *algoritmo* | *dim. blocco* | *dim. digest* | *documentazione* |
|---|---|---|---|
| MD2 | 8 bit | 128 bit | RFC-1319 |
| MD4 | 512 bit | 128 bit | RFC-1320 |
| MD5 | 512 bit | 128 bit | RFC-1321 |
| RIPEMD | 512 bit | 160 bit | ISO/IEC 10118-3 |
| SHA-1 | 512 bit | 160 bit | FIPS 180-1 RFC-3174 |
| SHA-224 | 512 bit | 224 bit | FIPS 180-2 RFC-4634 |
| SHA-256 | 512 bit | 256 bit | FIPS 180-2 RFC-4634 |
| SHA-384 | 512 bit | 384 bit | FIPS 180-2 RFC-4634 |
| SHA-512 | 512 bit | 512 bit | FIPS 180-2 RFC-4634 |

Tabella 3.1. Algoritmi di hash crittografici.

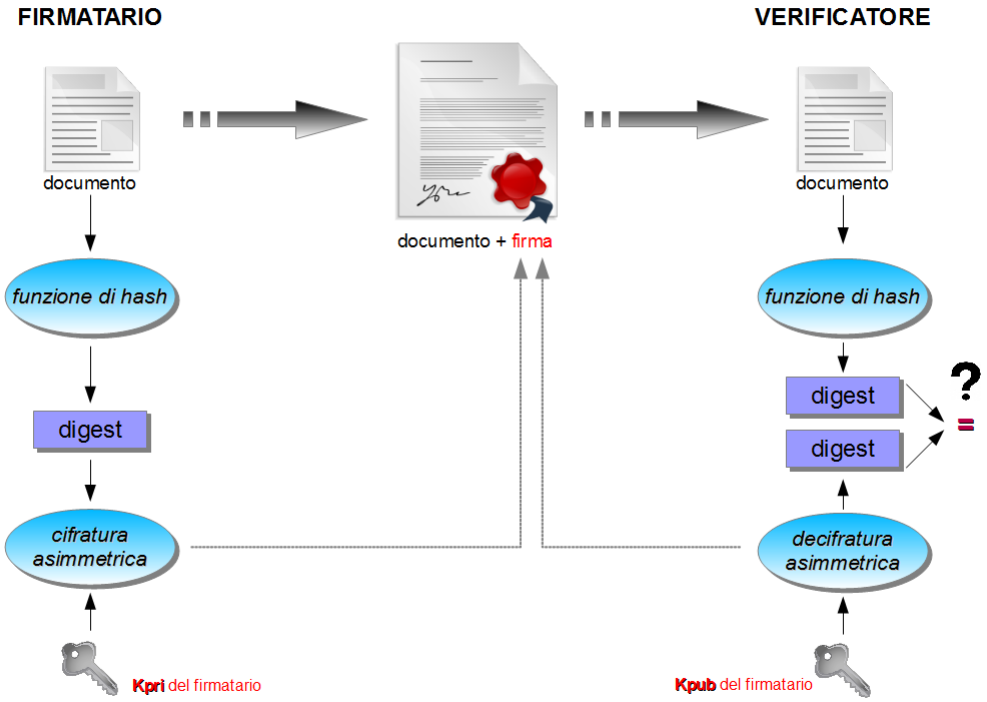


Figura 3.3. Creazione e verifica di una firma digitale.

1. il firmatario, che vuole generare una firma digitale, applica una funzione di hash al documento in chiaro;

2. il digest ottenuto (di lunghezza predeterminata) viene cifrato (mediante un algoritmo di cifratura asimmetrica) con la chiave privata (Kpri) del firmatario;

3. la stringa di bit prodotta dall'operazione di cifratura è detta **firma digitale**; questa viene accompagnata e distribuita assieme al documento;

4. qualsiasi soggetto voglia verificare la firma apposta al documento deve prima decifrarla con la chiave pubblica (Kpub) del firmatario che l'ha generata;

5. l'operazione di decifrazione restituisce un digest; questo viene quindi confrontato con quello generato a partire dallo stesso documento ricevuto dal soggetto verificatore;

6. la firma viene riconosciuta come valida se il confronto tra i due digest ha esito positivo (ossia i digest coincidono).

L'esito positivo del confronto permette in realtà di desumere una serie di importanti aspetti:

- la firma è valida ed è autentica (è stata quindi generata con la chiave privata del firmatario che ha apposto la firma al documento); ricordiamo però che, dal punto di vista normativo, la firma è valida inoltre se il firmatario dimostra di essere in possesso di un dispositivo sicuro di creazione di firma su cui ha il controllo esclusivo;
- il documento non è stato modificato dal momento in cui è stato firmato digitalmente; in caso contrario il digest generato dal verificatore non avrebbe coinciso con quello ottenuto dalla decifrazione della firma;
- la firma digitale è stata effettivamente decifrata con la chiave pubblica del firmatario.

Osserviamo quindi le possibili cause che possono portare ad avere digest diversi:

- *manipolazione dei dati* del documento nel passaggio da firmatario a verificatore;
- *sostituzione di firma*: la firma accompagnata al documento non è la stessa con cui il documento è stato in origine firmato;
- *scambio di persona*: si decifra la firma con un chiave pubblica diversa da quella posseduta dal firmatario.

La firma digitale si caratterizza come uno strumento legato in modo indissolubile ai dati; si noti che:

- la firma dipende dal firmatario e dal documento;
- poiché un firmatario non possiede una firma, ma al più una chiave privata, documenti uguali, firmati da soggetti diversi, hanno firme digitali diverse;
- documenti diversi firmati dallo stesso soggetto avranno firme digitali diverse.

Posto che la chiave privata è di proprietà esclusiva del firmatario, il problema che si presenta adesso è: come distribuire la chiave pubblica (che, come si è appena discusso, è necessaria qualora si voglia verificare la provenienza e l'integrità del documento)? La soluzione attualmente adottata è quella basata su un oggetto informatico chiamato *certificato*, a cui verrà dedicata la seguente sezione.

### 3.2.4 Il certificato

Un certificato è una struttura dati che comprova in modo univoco l'associazione tra una chiave pubblica ed alcuni attributi legati all'identità digitale di un soggetto (una persona, un nodo di rete, una società, ecc.), al quale tale chiave appartiene; il soggetto dichiara, mediante il certificato, di limitare l'utilizzo della chiave pubblica a specifici ambiti di sicurezza (cifratura asimmetrica, firma digitale, ecc.).

È rilasciato (mediante una procedura di certificazione) da un ente di terza parte (trusted third party) riconosciuto come autorità di certificazione (certification authority o, nel seguito, CA), che garantisce l'affidabilità dei dati ivi contenuti nonché la sua pubblicazione presso archivi digitali accessibili online. Gli enti di certificazione italiani che rilasciano certificati qualificati possono, secondo la normativa vigente, essere accreditati presso l'ente istituzionale che vigila sulle attività di certificazione (attualmente tale compito è svolto dall'Agenzia per l'Italia digitale).

È doveroso a questo punto fare una precisazione sulle tipologie di certificato e certificatore previste dalle attuali norme; riprendendo le definizioni presenti nella direttiva europea (sezione 2.3), in seguito recepite ed integrate nel CAD, distinguiamo due tipi di certificato:

- *certificati elettronici*: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche (nel nostro ambito i "dati utilizzati per verificare le firme" diventano semplicemente la chiave pubblica);
- *certificati qualificati (qualified certificate o QC)*: i certificati conformi ai requisiti di cui all'allegato I della direttiva europea, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della stessa direttiva; l'allegato I sancisce che il certificato qualificato, per essere tale, deve contenere una serie di informazioni aggiuntive come:
  - l'indicazione che si tratta di certificato qualificato;
  - l'indicazione del certificatore e dello stato in cui il certificatore è stabilito;
  - indicazioni sui limiti di utilizzo del certificato;
  - indicazioni sui limiti delle transazioni commerciali effettuabili con il certificato.

  L'RFC-3739 definisce il profilo dei certificati qualificati, conformi allo standard X.509 (che tratteremo in seguito).

I soggetti che rilasciano certificati si distinguono invece in:

- *certificatori qualificati*: coloro che rilasciano certificati qualificati e che devono possedere una serie di requisiti fondamentali che possiamo sintetizzare qui di seguito (allegato II della direttiva):
  - l'affidabilità (organizzativa, tecnica e finanziaria) necessaria per fornire servizi di certificazione;
  - capacità di verificare con mezzi appropriati l'identità del soggetto (nonché specifiche qualifiche) a cui è stato rilasciato il certificato;
  - capacità di determinare con precisione la data e l'ora di rilascio o di revoca di un certificato;
  - impiego di personale competente, quindi dotato di conoscenze specifiche ed esperienza necessari per erogare i servizi previsti;
  - utilizzo di sistemi affidabili e prodotti di firma conformi ai criteri di sicurezza riconosciuti e validi ai sensi delle norme vigenti;
  - capacità di instaurare una relazione contrattuale con il soggetto che ha richiesto i servizi di certificazione, tramite cui informarlo degli esatti termini e condizioni relative all'uso del certificato, ivi compresa ogni limitazione all'uso;
  - utilizzo di sistemi affidabili per la memorizzazione dei certificati attraverso a cui solo i soggetti autorizzati possono accedere e che consenta la verifica dell'autenticità dei dati che costituiscono il certificato.

  I certificatori qualificati (a differenza di quelli accreditati) non sono subordinati ad alcuna autorizzazione preventiva da parte dello Stato (l'attività dei certificatori stabiliti in Italia o in qualsiasi altro Stato membro dell'Unione Europea è dunque libera, secondo quanto stabilito dall'articolo 26 del CAD), ma devono comunque dare avviso di inizio attività al Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri [11]. Non esiste quindi un elenco pubblico dei certificatori qualificati, ma ciò non vieta ad un certificatore di fare istanza di notifica presso l'ente.
- *certificatori accreditati*: un certificatore qualificato che intenda disporre di maggiore visibilità sul mercato internazionale [11] deve fare una esplicita richiesta di accreditamento presso il dipartimento; il certificatore deve quindi dimostrare di godere di una serie di requisiti aggiuntivi a quelli già posseduti, in particolare (articolo 29, comma 3°):
  - se soggetto privato, deve avere natura giuridica di società di capitali con un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria;

– garantire il possesso di requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche [...].

Il certificatore accreditato è quindi inserito nell'elenco pubblico dei certificatori accreditati, consultabile per via telematica, gestito ed aggiornato dall'Agenzia per l'Italia digitale (ex DigitPA); il certificatore è soggetto ad attività di vigilanza da parte di questo ente.

### 3.2.5 Formato X.509

Il formato X.509 è uno standard pubblico ITU-T, fondamentale per il funzionamento delle infrastrutture a chiave pubblica (public key infrastructure o PKI) ed è attualmente il più diffuso nella pratica per i certificati a chiave pubblica; parte integrante dello standard X.500, il formato X.509 (versione 3) definisce le specifiche della struttura dati che rappresenta il certificato, gli attori coinvolti nel sistema di infrastruttura a chiave pubblica e le modalità con cui le CA forniscono servizi di certificazione ai soggetti che ne fanno richiesta.

Come descritto nella RFC-3280, un certificato è una sequenza di tre campi fondamentali (verrà fornita una descrizione semplificata, che non fa riferimento alla ASN[5] adottata invece nella rfc):

- tbsCertificate (il certificato da firmare);
- signatureAlgorithm (l'algoritmo di firma del certificato);
- signatureValue (la firma apposta al certificato).

#### tbsCertificate

Il campo che rappresenta il certificato è composto a sua volta da una serie di campi:

- *version*: questo campo descrive la versione del certificato codificato; se il certificato comprende anche le estensioni, allora la versione indicata deve essere v3; se non sono presenti estensioni, la versione dovrebbe essere v2 (ma può essere anche v3);
- *serial number*: un numero positivo intero assegnato dalla CA a ciascun certificato; deve essere univoco per ogni certificato emesso da una CA; il numero non deve eccedere i 20 ottetti di lunghezza;
- *signature*: questo campo contiene l'algoritmo di firma utilizzato per firmare il certificato; la descrizione deve includere l'identificativo dell'algoritmo di cifratura, unito ad una serie di parametri opzionali che variano in base all'algoritmo stesso (es. RSA with MD5, 1024); questo campo deve coincidere con il campo signatureAlgorithm della struttura principale;
- *issuer*: identifica l'ente che ha firmato ed emesso il certificato; questo campo contiene un set di attributi standard (alcuni opzionali, altri obbligatori come il *distinguished name* (DN)):
  - country;
  - organization;
  - organization-unit;
  - distinguished name qualifier;
  - state or province name;
  - common name;
  - serial number.

[5] Abstract Syntax Notation.

- *validity*: questo campo fornisce indicazioni circa l'intervallo temporale nel quale la CA garantisce la validità delle informazioni contenute nel certificato; si compone di due date: la prima si riferisce all'istante di inizio validità del certificato (es. 01/01/2012), la seconda invece decreta la fine della validità (es. 31/12/2012);
- *subject*: l'entità associata alla chiave pubblica contenuta nell'omonimo campo del certificato (nonché la stessa che controlla la corrispondente chiave privata); il subject può anche essere una CA (in tal caso il campo deve contenere un distinguished name);
- *subjectPublicKeyInfo*: questo campo trasporta la stringa di bit della chiave pubblica ed identifica l'algoritmo con cui la chiave è usata (es. RSA, 1024).

**signatureAlgorithm**

Questo campo contiene l'identificativo dell'algoritmo di cifratura (e relativi parametri) usato dalla CA per firmare questo certificato; deve coincidere con il campo signature della struttura tbsCertificate.

**signatureValue**

Questo campo contiene una firma digitale calcolata sul certificato; codificata come stringa di bit, la firma digitale è il mezzo con cui la CA convalida il certificato e l'associazione tra la chiave pubblica e il soggetto indicato nel campo subject.

## 3.3 Firma biometrica grafometrica

Prima di analizzare nel dettaglio questa *species* di firma elettronica, la sua collocazione nell'attuale panorama normativo e le modalità con cui si adopera, è opportuno approfondire gli aspetti tecnici principali che regolano la biometria e le tecnologie biometriche in particolare.

### 3.3.1 Processo biometrico

La biometria e le sue applicazioni tecniche rappresentano ad oggi un valido strumento con cui sviluppare soluzioni di sicurezza avanzate, il cui funzionamento consiste principalmente nella identificazione o verifica automatica dell'identità degli individui; ciò avviene attraverso il riconoscimento e la valutazione di precise caratteristiche fisiche e comportamentali dell'individuo stesso[6].

Supportate da una diffusione sempre crescente soprattutto nel settore delle amministrazioni pubbliche (si pensi ad esempio alla necessità di controllare l'accesso fisico a determinate aree riservate di edifici o l'accesso logico ad alcune risorse informatiche protette), che ne giustifica un utilizzo quasi pervasivo (con le ovvie conseguenze sulla privacy che ne derivano), le tecnologie biometriche non sono tipicamente adottate come strumento esclusivo con cui fare sicurezza, bensì sono parte integrante di una soluzione più ampia che include altre tecnologie orientate all'identificazione sicura.

In questa sezione verrà spiegato in dettaglio il processo biometrico attraverso cui vengono acquisite prima ed impiegate poi le informazioni biometriche di cui si accennava. Le fasi di un processo biometrico possono essere sintetizzate nelle tre seguenti:

1. Registrazione (o enrollment);

[6] Le caratteristiche comportamentali in particolare saranno oggetto della nostra discussione.

2. Verifica;
3. Identificazione.

Prenderemo come riferimento la figura 3.4:

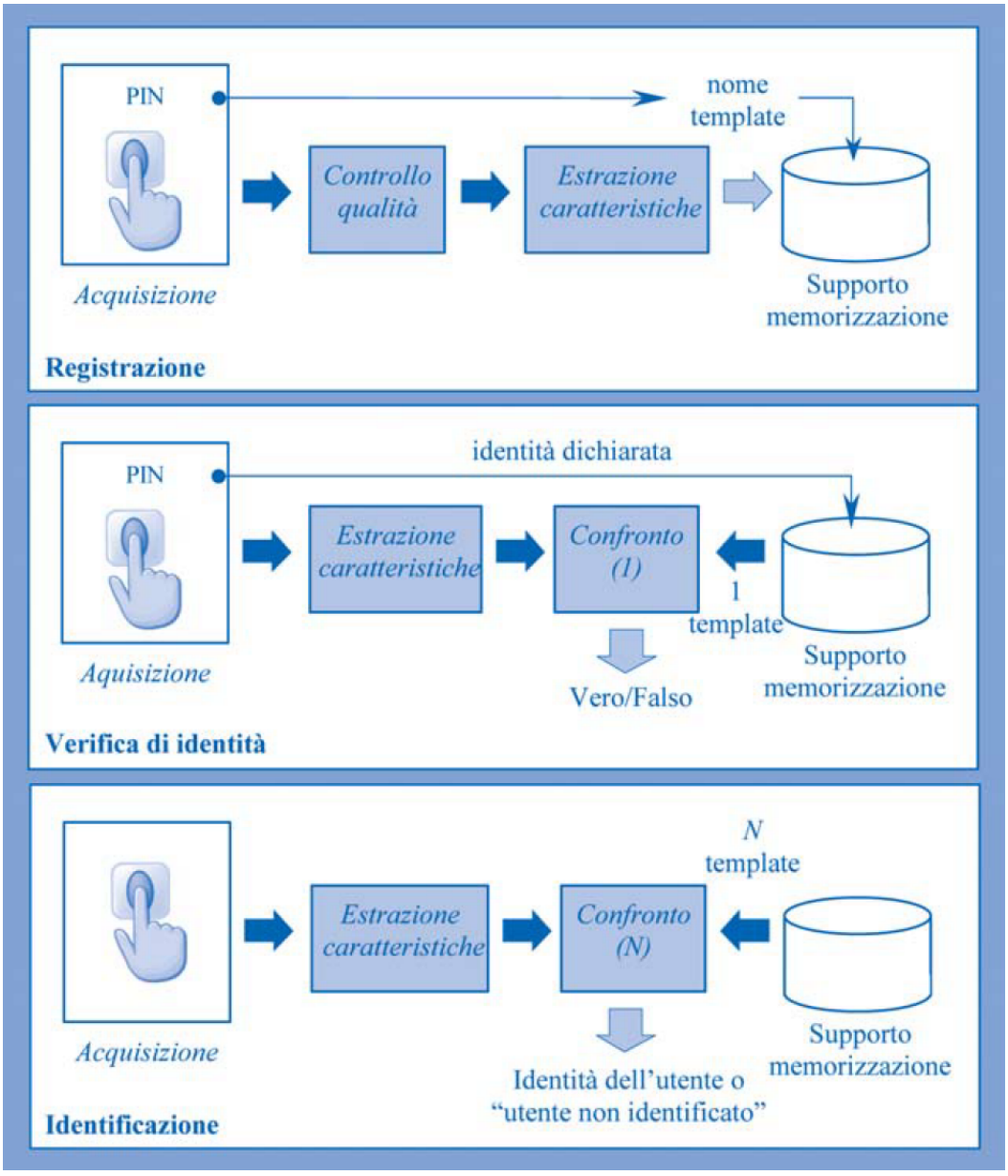


Figura 3.4. Fasi di un processo biometrico (fonte: CNIPA, i "Quaderni" n. 9 (novembre 2004)).

### Registrazione

La registrazione è la prima fase del processo e consiste nell'acquisizione (da parte di un sensore biometrico) e nella successiva memorizzazione delle caratteristiche biometriche dell'individuo. Le caratteristiche non sono generalmente archiviate in modo grezzo, ma dal cosiddetto "campione biometrico" viene estratta una certa quantità di informazioni numeriche, che prende il nome di *template*. Per esigenze di maggiore precisione ed affidabilità è possibile che il campione venga

rilevato più volte prima di procedere con la registrazione del template. Quest'ultimo viene quindi immagazzinato in un supporto di memorizzazione non volatile e recuperato soltanto in fase di verifica o identificazione.

Questa fase attribuisce una **identità biometrica** al soggetto che si è registrato; data la criticità dell'operazione, tipicamente viene preventivamente richiesto al soggetto l'esibizione di un documento d'identità o altro strumento che ne avvalori la titolarità, affinché si proceda con la registrazione vera e propria; data la sensibilità dei dati da registrare, questi vengono comunemente salvati su un dispositivo sicuro, ad uso e controllo esclusivo del legittimo fruitore.

#### Verifica

Questa è la fase responsabile della verifica dell'identità dell'utente, che deve coincidere con quella ottenuta nello stadio di registrazione. Il sensore biometrico acquisisce il campione biometrico, quindi viene generato il template relativo; segue un'operazione di confronto tra questo template e quello precedentemente ottenuto in fase di registrazione, memorizzato su un dispositivo sicuro.

La fase di verifica si distingue da quella di identificazione per la necessità di indicizzare il template registrato con una informazione aggiuntiva a conoscenza dell'utente (ad esempio un PIN). Il confronto determina un esito, positivo o negativo in base al grado di coincidenza valutato tra i due template.

#### Identificazione

La fase di identificazione non prevede l'utilizzo di dispositivi che contengano le informazioni biometriche né l'indicizzazione del template registrato; il confronto avviene tra il template appena generato con tutti quelli presenti nel sistema, al fine di individuare un "template simile" (secondo determinati parametri di valutazione) e verificare quindi correttamente l'identità dell'individuo.

### 3.3.2 Il riconoscimento biometrico della firma

Le tecniche adottate in ambito biometrico sono ad oggi varie e molteplici: si va dalla rilevazione delle impronte digitali al riconoscimento biometrico del volto e della voce; scopo di questa sezione è introdurre la tecnologia legata al riconoscimento biometrico della firma ed i principi biometrici di base che ne governano il funzionamento.

Il processo di apposizione di una firma su un documento ben si colloca in un contesto di generazione di caratteristiche biometriche univoche e peculiari dell'individuo firmatario: come argomentato in [12], la firma può essere considerata ragionevolmente univoca per una serie di caratteristiche quali la velocità di scrittura, intensità e frequenza di punti di pressione esercitati, ecc.; queste rientrano nella categoria delle **caratteristiche biometriche comportamentali** di un utente e sono associate univocamente ad un individuo, in quanto difficilmente riproducibili.

La proprietà distintiva di tali parametri e la facilità con cui è possibile impiegarli nella realtà quotidiana rendono il riconoscimento biometrico della firma un approccio interessante allo sviluppo di soluzioni non solo in ambito amministrativo, ma anche bancario e finanziario [12]:

> Il riconoscimento biometrico della firma gode di una certa popolarità negli ambienti bancari e finanziari in cui l'apposizione della firma è una prassi frequente e, senza richiedere un cambio delle abitudini da parte dell'utente o un particolare addestramento, permette un considerevole incremento di sicurezza

#### Parametri biometrici di firma

Nella dinamica di apposizione di una firma individuiamo i principali parametri di riconoscimento biometrico:

- Posizione della penna durante il movimento;
- Durata del processo di firma;
- Pressione esercitata;
- Velocità di scrittura;
- Accelerazione del movimento.

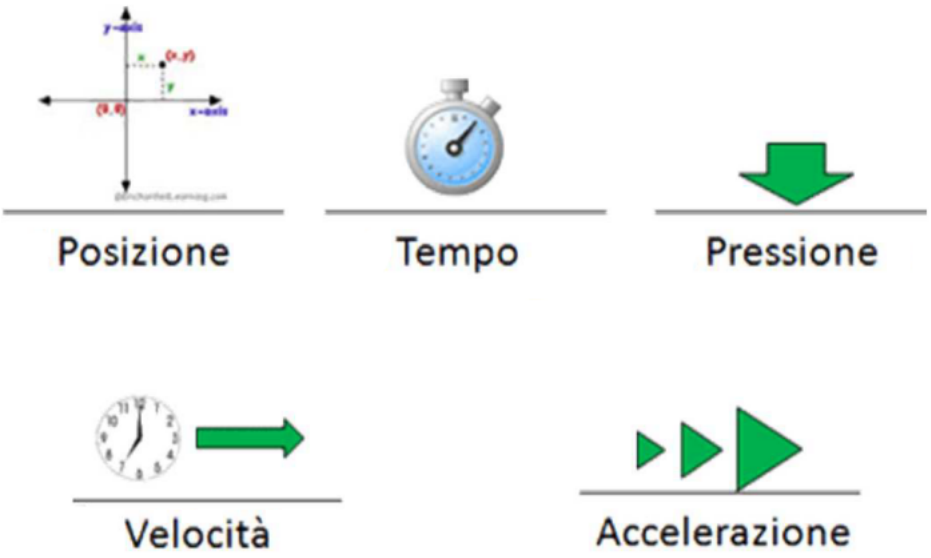


Figura 3.5. Alcuni parametri di firma.

La misurazione di questi cinque parametri consente di identificare, in maniera pressoché univoca, una **firma grafometrica** (conosciuta anche come firma biometrica grafometrica o, più semplicemente, firma biometrica), realizzata mediante l'utilizzo di dispositivi come *tablet* (o tavoletta elettronica) su cui l'utente esercita i movimenti tipici di una scrittura autografa su carta. Il dispositivo in questione deve ovviamente disporre della tecnologia necessaria (ad esempio uno schermo sensibile alle variazioni delle intensità di pressione) per rilevare i parametri biometrici sopracitati.

Esistono tuttavia alcune criticità legate alla loro verifica, non certa ed affidabile del tutto, ma soggetta a una soglia di accettazione che viene determinata da due parametri:

- FAR (False Acceptance Rate): percentuale del numero di accettazioni di una firma non valida (caso in cui è riconosciuto come valido un campione biometrico che invece non lo è);
- FRR (False Rejection Rate): percentuale del numero di rifiuti di firme valide (caso in cui è riconosciuto come non valido e quindi falso un campione biometrico che invece non lo è).

La calibrazione della soglia di accettazione dei dati dipende quindi da questi due valori, che misurano di fatto la bontà del riconoscimento biometrico; essi sono in parte modificabili, ma dipendono principalmente dalle caratteristiche e dalla qualità del dispositivo di rilevazione (figura 3.6).

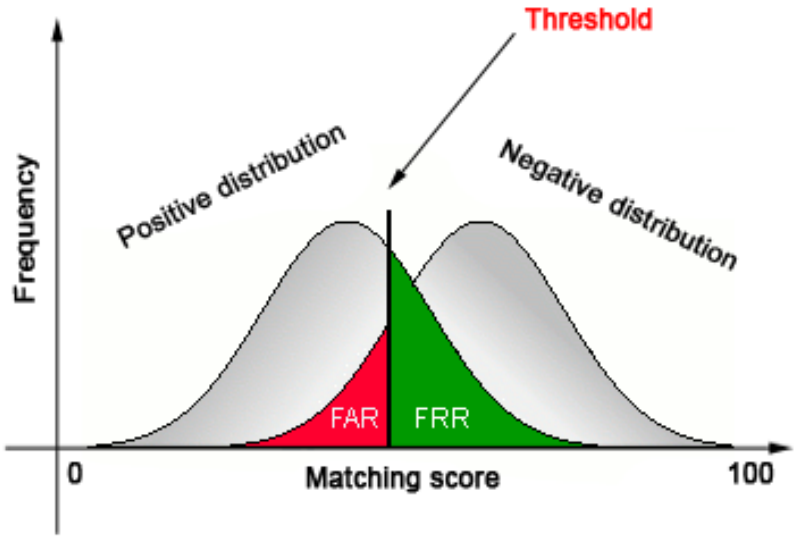


Figura 3.6. FAR, FRR e soglia di accettazione (threshold).

### 3.3.3 Scenari applicativi

Come già accennato in 3.3.2, il processo di generazione di una firma biometrica prevede che dal dispositivo con cui si appone la firma sia possibile estrarre determinati parametri biometrici appartenenti alla sfera comportamentale dell'individuo firmatario: in altri termini, la firma biometrica apposta ad un documento informatico non è la semplice scansione digitale della firma autografa; questo particolare tipo di firma prende il nome di **firma elettronica autografa**, di fatto una firma "digitalizzata".

Da considerare inoltre che gli stessi dati biometrici di firma ed il loro utilizzo non soddisfano appieno i requisiti di firma elettronica avanzata (sezione 2.4.4, definizione di FEA nel CAD) in quanto, sebbene possano assolvere al requisito di identificazione del firmatario, non possono garantire la connessione univoca della firma al firmatario, né la verifica dell'integrità dello stesso documento; il requisito di associazione può essere rispettato se il firmatario dispone di un tablet su cui ha un controllo esclusivo e con il quale generare firme grafometriche; è possibile quindi realizzare una firma grafometrica che sia, ai sensi della normativa, una FEA e che ne rispetti i requisiti sanciti dalla definizione, ma ad oggi non è ancora disponibile la stesura definitiva del decreto attuativo che riguarda la FEA, di conseguenza una firma grafometrica in quanto tale è da intendersi come semplice firma elettronica.

Le modificazioni al CAD del 2010 (che recepiscono integralmente la direttiva europea in merito alle firme elettroniche avanzate e assegnano ad esse piena validità giuridica) assegnano tuttavia una nuova efficacia alle firme grafometriche se assistite da un processo di firma digitale che, rispettando comunque i requisiti oggettivi e soggettivi indicati nelle regole tecniche, definisce nel complesso una soluzione di FEA valida ai sensi di legge.

Qui di seguito verranno proposti due scenari applicativi che mostrano alcune realtà di utilizzo delle tecnologie biometriche e le modalità con cui esse si combinano alla firma digitale.

#### PKI e autenticazione biometrica

Si è già accennato nella sezione 3.2.5 all'infrastruttura a chiave pubblica (nota come PKI), che determina l'insieme di procedure, processi e tecnologie di cifratura asimmetrica adoperate per lo

sviluppo di applicazioni distribuite di firma digitale, conservazione e scambio di certificati digitali, ecc. In un contesto di firma digitale, si sono anche affrontati i possibili modi di generazione delle chiavi usate per cifrare e decifrare i documenti firmati digitalmente, indicando in particolare l'opzione attualmente più utilizzata, ossia quella che prevede la generazione e la conservazione delle chiavi (nonché del certificato ad esse collegato) all'interno di un dispositivo di firma (si veda la sezione 3.2.1).

Il *dispositivo di firma* diventa dunque lo strumento attraverso il quale un utente abilitato può generare e successivamente apporre su un documento una firma digitale; la normativa vigente prevista dal CAD richiede in realtà che il dispositivo sia anche sicuro, condizione necessaria data la sensibilità delle informazioni che devono essere protette (chiave privata in primis), di conseguenza:

> Il titolare del certificato di firma 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; è altresì tenuto ad utilizzare personalmente il dispositivo di firma

Ora, l'accesso esclusivo al dispositivo può essere realizzato scegliendo tra due modalità [13]:

- verifica di una cosa che il sottoscrittore conosce (tipicamente un numero identificativo o PIN, o una password);
- verifica di una caratteristica biometrica del sottoscrittore.

La tecnologia biometrica diventa determinante nella seconda opzione, come strumento di *strong authentication* della firma digitale; tale opzione richiede infatti una preventiva registrazione dei dati biometrici comportamentali del firmatario e quindi un controllo di accesso al dispositivo che passa da una verifica tra template registrato ed acquisito, come spiegato in 3.3.1.

Questa procedura di autenticazione basata sulla biometria prende il nome di *match-on-card* e risolve alcune criticità legate alla prima opzione, garantendo un elevato grado di sicurezza: non essendo più richiesta l'adozione di un PIN, il rischio associato al suo furto o intercettazione viene meno; tutte le informazioni legate al template biometrico sono memorizzate nel dispositivo, che ne protegge l'integrità; nessuna informazione è resa disponibile a terzi.

La configurazione hardware del dispositivo deve essere opportunamente adeguata a questo nuovo scenario: deve quindi disporre di un sensore biometrico per la registrazione dei modelli di firma dell'utente e anche di un coprocessore per il confronto tra i template.

L'infrastruttura deve considerare anche l'adozione di nuovi standard che garantiscano l'interoperabilità tra i vari ambienti (ad esempio, occorre standardizzare la codifica e la struttura dei dati biometrici) [13].

#### Firma biometrica e firma digitale: una soluzione di FEA

Soltanto di recente (dicembre 2010, con le modifiche ed integrazioni al CAD) la normativa italiana ha ripreso le disposizioni sancite dalla direttiva europea riguardanti la firma elettronica avanzata, riconoscendone pienamente il ruolo nel contesto delle firme elettroniche; la firma elettronica avanzata, ricordiamo, è un particolare tipo di firma elettronica che si differenzia da quest'ultima per ulteriori caratteristiche di sicurezza che ne forniscono pieno valore giuridico ai sensi di legge, in quanto deve garantire:

- l'identificazione del firmatario del documento;
- la connessione univoca della firma al firmatario;
- il controllo esclusivo del firmatario del sistema di generazione della firma;
- la possibilità di verificare che il documento non abbia subito modifiche dopo l'apposizione della firma;

- la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
- l'individuazione del soggetto che ha erogato il servizio di firma elettronica avanzata.

Come già spiegato in precedenza, a differenza delle firme qualificate, le firme elettroniche avanzate non sono legate ad una tecnologia specifica che risponde a determinati requisiti di sicurezza, ma costituiscono un **processo** o **soluzione di firma**; sarà quindi necessario valutare, caso per caso, se la soluzione presentata soddisfa i requisiti sopracitati e se quindi può costituire una soluzione di firma elettronica avanzata.

È già stata data una definizione di firma grafometrica, ovvero di una firma elettronica ottenuta mediante la rilevazione e l'elaborazione di dati biometrici comportamentali (o parametri calligrafici) di firma tramite dispositivi tablet; il processo di generazione, apposizione e verifica di una firma grafometrica per come è stato descritto nelle sezioni precedenti non è idoneo a garantire le proprietà di cui sopra, e la mancanza di una versione definitiva delle regole tecniche per la firma elettronica avanzata (che indichi in modo univoco le modalità operative per cui una firma biometrica grafometrica possa costituire una FEA) di fatto la pone nella categoria più ampia delle firme elettroniche.

La facilità e la naturalezza con cui un firmatario appone una firma su tablet (esercitando i consueti movimenti della mano tipici della sottoscrizione autografa) determina un'alta accettazione da parte degli utenti per la firma grafometrica e per l'utilizzo di dispositivi elettronici di firma, nonché una esigenza sempre crescente di dotare tale tipo di firma delle caratteristiche necessarie per trovare ampia applicabilità pratica.

La connotazione generale della definizione della FEA consente di realizzare una soluzione che integri la firma grafometrica con altri tipi di firme che soddisfino i requisiti già citati e si avvalgano delle caratteristiche "user-friendly" della prima, per sviluppare processi che superino il "digital-divide".

La soluzione presentata qui di seguito (e riconsiderata nel capitolo 4) è una tipica soluzione di firma elettronica avanzata e prevede l'integrazione del processo di generazione di una firma grafometrica con quello di firma digitale: si parlerà quindi di una soluzione di firma elettronica avanzata basata su dati biometrici (figura 3.7).

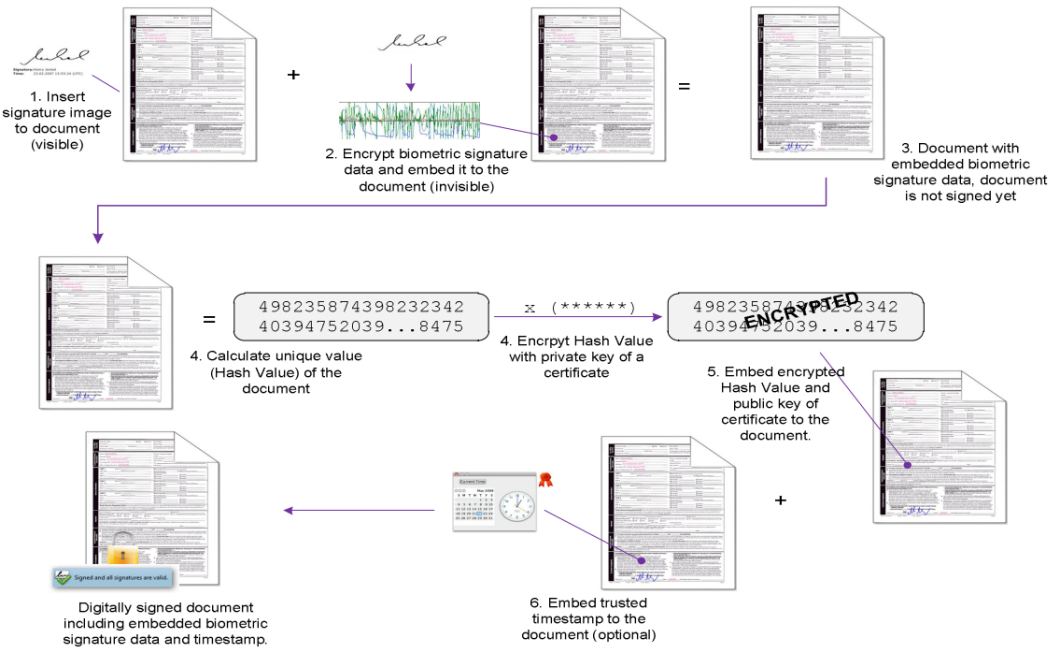


Figura 3.7. Firma elettronica avanzata con dati biometrici (fonte: Forum PA 2012, In.Te.S.A. S.p.A.).

Sia dato un documento e lo si voglia firmare elettronicamente; l'utente, verificato il documento da sottoscrivere, interagisce con il tablet di firma collegato alla postazione di lavoro (computer e tablet comunicano mediante un apposito software) ponendo la propria firma autografa quando richiesto; eseguita la firma (ed acclarata dall'utente, il quale può eventualmente decidere di rieseguire l'operazione, annullando la precedente), il documento viene sottoposto ad un processo che si compone dei seguenti passi (si prenda a riferimento sempre la figura 3.7):

1. L'immagine della firma autografa dell'utente viene inserita in un'area del documento (impostata tramite software) e resa visibile in fase di visualizzazione;
2. Il tablet estrae i dati biometrici comportamentali sulla base della dinamica della firma e genera il corrispondente template numerico; questo viene quindi cifrato ed incorporato nel documento (né i parametri calligrafici né il template cifrato sono visibili nel documento);
    - la chiave con cui si effettua la cifratura (ed eventuale decifratura da parte di grafologi per contenziosi sulla paternità della firma) viene in questo contesto chiamata *master key*, custodita in un ambiente sicuro (tipicamente l'HSM dello stesso tablet);
    - per proteggere i dati biometrici da eventuali attacchi, questi vengono cifrati il prima possibile, in genere direttamente sul tablet; ciò consente di ridurre notevolmente l'esposizione dei dati sensibili e garantisce che possano essere disponibili all'esterno del dispositivo sempre cifrati.
3. Il risultato dei primi due punti è un documento a cui sono stati associati i dati cifrati della firma grafometrica e su cui è visibile la firma dell'utente (questo aspetto dota il documento digitale delle stesse caratteristiche di *look and feel* del documento cartaceo su cui è stata apposta in calce la firma autografa, producendo un'elevata accettabilità del sistema da parte del firmatario);
4. Viene quindi generato un hash value (digest) del documento considerato, cifrato con la chiave privata di un certificato; occorre a questo punto fare delle precisazioni:
    - la firma del documento avviene con la tecnica delle chiavi asimmetriche; la firma generata è quindi una firma digitale (si vedano le sezioni 2.4.6 e 3.2);
    - il certificato digitale (sezione 3.2.4) contenente la chiave pubblica associata a quella privata è "auto firmato" (*self signed*); i certificati adoperati nelle soluzioni di firma elettronica avanzata sono generalmente self signed, perché questo evita di dover disporre di infrastrutture complesse (come ad esempio le PKI) per la generazione e la distribuzione dei certificati.
5. Il risultato della cifratura del digest viene incorporato nel documento insieme alla chiave pubblica del certificato (servirà per una verifica di integrità del documento);
6. Viene generata ed apposta al documento opzionalmente anche una marca temporale (indica l'istante di apposizione della firma digitale ed è obbligatoria in caso di conservazione sostitutiva del documento; si veda la sezione 3.1 per maggiori approfondimenti).

La soluzione di firma elettronica avanzata presentata produce un documento firmato sia con una firma biometrica che con una firma digitale.

# Capitolo 4

# SOFTPRO SDK

Fatte le dovute considerazioni nel capitolo 3 sulle caratteristiche della firma digitale prima e della firma biometrica grafometrica poi (nel seguito si adotterà semplicemente il termine grafometrica), i successivi capitoli sono interamente dedicati all'analisi ed alla progettazione di una soluzione di firma elettronica avanzata, in particolar modo un'applicazione client stand-alone in ambito desktop che integri i concetti già espressi nelle precedenti sezioni ed interagisca con un dispositivo di firma per l'acquisizione della firma stessa da parte dell'utente firmatario.

Per la realizzazione applicativa ci si è basati su un insieme di strumenti di sviluppo (SDK, Software Development Kit) messi a disposizione dalla società **Softpro GmbH**, grazie ad un accordo (NDA, Non-disclosure agreement) siglato tra la stessa Softpro e la Consoft Sistemi S.p.A. che ne configura l'utilizzo entro certi limiti temporali.

Il seguente capitolo offre una panoramica generale degli strumenti software adoperati per l'implementazione del processo di firma elettronica avanzata (per la cui analisi si rimanda ai capitoli 5 e 6), nonché dei principali dispositivi di firma presenti ad oggi sul mercato (uno dei quali sarà preso come riferimento per lo sviluppo del processo stesso).

## 4.1 SOFTPRO

La Softpro GmbH [14] è una società, fondata nel 1983 con sede principale in Germania, specializzata nello sviluppo di processi affidabili di firma elettronica su workflow digitali. La Softpro sviluppa e vende sul mercato strumenti, prodotti e soluzioni per la cattura di firme elettroniche, la gestione all'interno di un workflow aziendale ed infine la loro verifica. Nel 2011 è stata riconosciuta come leader mondiale nel campo del *signature management* [15]. I segmenti di mercato su cui la Softpro è maggiormente presente sono:

- assicurazioni;
- vendita al dettaglio;
- settore sanitario;
- settore amministrativo;
- telecomunicazioni.

Le attività fondamentali (core business) della società possono essere classificate in due categorie:

1. *E-Signing*: soluzioni per l'acquisizione di firme elettroniche e la loro apposizione su documenti digitali (**eSWS**, Electronic Signature Workflow Solutions), che spaziano da applicazioni software desktop ad intere piattaforme web-based, compatibili con un ampia varietà di dispositivi progettati per il signature capturing;

2. *Signature Verification*: suite di soluzioni per la prevenzione di frodi (FPS, Fraud Prevention Solutions).

La nostra soluzione di FEA appartiene alla prima categoria.

### 4.1.1 E-signing: la firma elettronica avanzata secondo Softpro

Le soluzioni eSWS targate Softpro si collocano in tutte quelle realtà che pongono come obiettivi principali il:

- risparmio dei costi;
- miglioramento della customer service.

Appare quindi evidente che le eSWS trovano applicabilità in processi di business come:

- gestione prelievo e deposito di contante, bonifici bancari, ecc.;
- generazione ordini di acquisto o vendita di beni;
- gestione pratiche amministrative;
- stipula contratti tra privati;
- consenso al trattamento dei dati personali;
- ...

Tali processi trovano ampio beneficio, in termini di risparmio, dalla eliminazione dei costi di gestione dei documenti cartacei, a favore dell'impiego e della distribuzione di documenti digitali nativi, firmati digitalmente; lo scambio documentale delle informazioni avviene mediante mezzi di comunicazione digitali connessi alla rete e con l'affidabilità di una firma elettronica sicura.

Il potenziale risparmio dovuto all'abbandono della carta nel processo di archiviazione e gestione dei documenti firmati con sottoscrizione autografa può essere facilmente intuito osservando come alcuni passi di un processo di business tradizionale possano in realtà essere considerati superflui e quindi eliminabili: stampa, preparazione del documento, apposizione di firma autografa, scansione, trasmissione, archiviazione, ecc.

Il nuovo processo si caratterizza per un miglioramento generale della qualità del servizio (figura 4.1); come evidenziato dalla figura, il processo a sinistra si compone di una serie di step quali la definizione, la gestione e la distribuzione di documenti fisici tra i diversi attori del processo (vendor e customer), nonché la scansione per una successiva archiviazione digitale; l'intero processo è principalmente condizionato dalla necessità di produrre grandi quantità di cartaceo che influiscono sui costi di gestione e trattamento delle stesse; a ciò andrebbe aggiunto anche l'impatto ambientale che deriva da un errato smaltimento della carta. Il nuovo processo (a destra della figura) adotta un sistema di creazione e gestione di documenti digitali nativi, firmati elettronicamente e distribuiti e verificati digitalmente; la scelta della firma elettronica creata a partire dalla sottoscrizione mediante tablet dota il processo delle caratteristiche (*user-friendly*) di alta usabilità ed accettazione da parte dell'utente, che si ritrova ad esercitare gli stessi comportamenti in entrambi i processi, non modificando quindi il proprio ruolo o le proprie responsabilità nel passaggio da un sistema all'altro.

Qui di seguito gli estratti di due conferenze che stimano i margini di risparmio e il ROI[1] derivanti dall'introduzione dell'E-signing presso la Cassa di Risparmio spagnola ([17]):

[1] Return On Investment.

Savings per document are expected to be at least 0.30 Euro per document. If E-Signing with Handwritten Signatures is fully in place in the Spanish Savings Banks this means savings near 300 Million Euros per year

E:

The average Spanish Savings Bank achieved the Return on Investment for implementing E-Singing below 11 months


Figura 4.1. Processi di business a confronto (fonte: E-Signing Overview).

È opportuno ricordare che la Germania è stato uno dei primi paesi della UE (contestualmente all'Italia) a recepire la direttiva europea (vedi 2.3) sulle firme elettroniche e quindi uno dei primi stati ad accogliere il dualismo tra firme elettroniche leggere e firme forti (si riprenda a tal proposito la sezione 2.4.7).

Tra le eSWS sviluppate, la principale, *SignDoc*, soddisfa la definizione di "advanced electronic signature" (ossia FEA) [16]; si tratta infatti di una soluzione caratterizzata da un valore probatorio pari a quello delle firme autografe apposte su un documento cartaceo, conforme ai requisiti delineati nella direttiva, ossia affidabilità, strong authentication del firmatario e possibilità di verifica dell'integrità del documento firmato, a seguito di successive modifiche (sezione 2.4.4). La normativa tedesca risulta essere quindi conforme con quanto sancito dalle disposizioni internazionali.

Si è fatta menzione della soluzione SignDoc perché realizzata con gli strumenti di sviluppo messi a disposizione dalla società, gli stessi a cui faremo riferimento nella progettazione della nostra soluzione e di cui si darà una descrizione generale nella prossima sezione.

### 4.1.2 Strumenti di sviluppo (SDK)

La Softpro colloca sul mercato un'ampia gamma di soluzioni per l'E-signing, compatibilmente con le diverse esigenze e necessità dei clienti. Esse si collocano principalmente nell'area *desktop* e *web*.

Si è accennato a SignDoc, l'implementazione di riferimento della società, distribuita per l'appunto nelle versioni *SignDoc Desktop* e *SignDoc Web*, nonché nella versione dedicata all'ambito dei dispositivi mobili, ossia *SignDoc Mobile*. Le loro funzionalità non si limitano al solo processo di firma (che comunque costituisce la feature principale), ma permettono una serie di operazioni aggiuntive, quali ad esempio:

- gestione di documenti in differenti formati (in primis PDF[2] e TIFF[3]), nonché la loro conversione a partire da formati chiusi (DOC, DOCX, XLS, XLSX) attraverso un sistema integrato;
- inclusione ed embedding di allegati al documento da firmare (ad esempio, scansione di documenti di identità o passaporti), operazione tipicamente utile nella redazione di contratti telefonici o per l'apertura di conti bancari;
- inserimento di foto o immagini associate al firmatario come parte della firma elettronica: in altri termini, possibilità di associare (*embed*) una foto o una immagine acquisita da una built-in camera ad un campo di firma del documento; questa opzione non costituisce certo elemento di sicurezza ulteriore, ma contribuisce ad aumentare la *trustworthiness* (affidabilità o attendibilità) della firma da parte del destinatario del documento;
- integrazione di certificati digitali: si è già discusso nella sezione 3.3.3 come l'integrazione del processo di firma grafometrica con la tecnica di firma digitale permetta la realizzazione di una soluzione di firma elettronica avanzata avente pieno valore legale e che nel contempo svincoli l'utente dall'onere di trattare informazioni sensibili (si pensi a PIN o password segrete) con cui accedere agli strumenti di firma (dispositivi come token usb o smart card contenenti chiavi di crittografia, ecc.), il cui furto o la cui manomissione da parte di malintenzionati possa compromettere la sicurezza della firma stessa;

  in un contesto di FEA, la grafometria ha il vantaggio di non imporre ostacoli artificiali al processo di firma, consentendo all'utente di governare l'intero procedimento attraverso l'interazione con il dispositivo di firma (esso conterrà tutti gli elementi necessari allo scopo, ossia certificati e chiavi, simmetrica e asimmetriche);

  la soluzione SignDoc permette la gestione e la configurazione dei certificati digitali (tipicamente self signed, per non dover adottare infrastrutture come la PKI per la generazione e la distribuzione dei certificati, come già detto nella sezione 3.3.3, ma ciò non vieta di adottare certificati validi rilasciati da terze parti); il documento firmato conterrà, oltre ai dati cifrati, anche il certificato e con esso la chiave pubblica associata, secondo modalità di imbustamento che verranno maggiormente approfondite nel seguito.

Tutte le applicazioni Softpro sono basate sui seguenti SDK:

- **SignDoc SDK**;
- **SignWare SDK**.

Insieme definiscono complessivamente la libreria software per le firme biometriche (che va sotto il nome di SignWare) da cui si sviluppa l'intera suite di programmi, come indicato in figura 4.2.

[2]Portable Document Format, formato proprietario di Adobe System, rilasciato e pubblicato come standard ISO 32000-1:2008. SignDoc Desktop è compliant con questo standard.

[3]Tagged Image File Format, o semplicemente TIF.

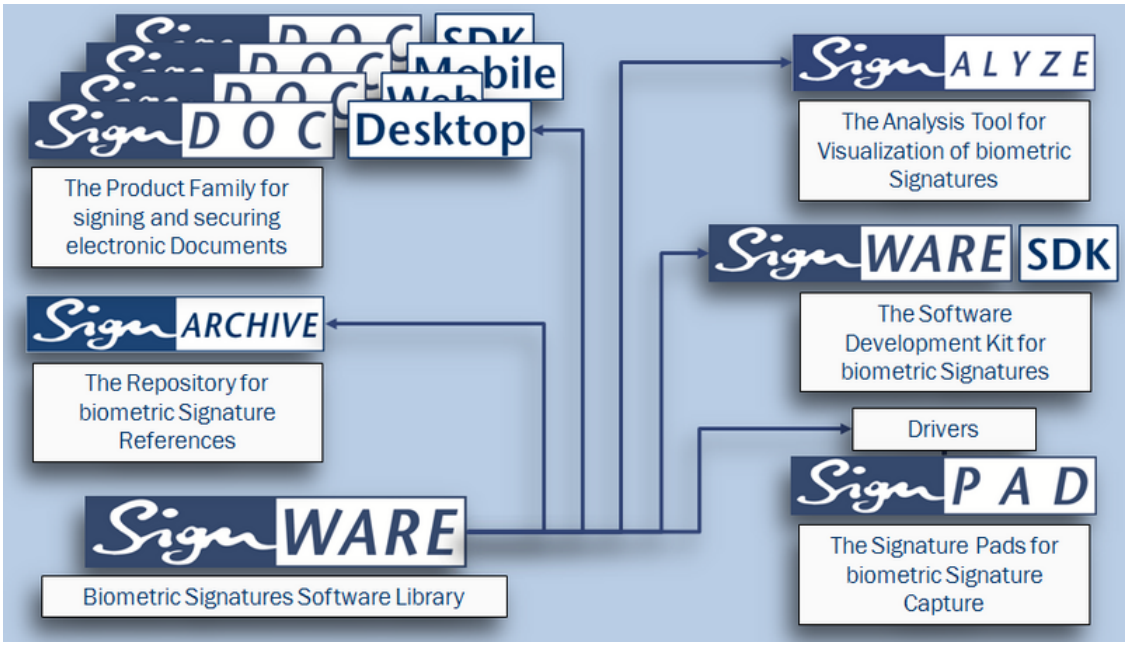


Figura 4.2. SignWare, SignDoc SDK e SignWare SDK (fonte: SOFTPRO Products build with SignWare).

### SignDoc SDK

Questo kit di sviluppo fornisce allo sviluppatore una serie di API[4] dedicate all'integrazione dell'E-signing nei documenti digitali; sono presenti quindi funzioni relative alla cifratura e alla generazione di hash value, procedure per la configurazione dei parametri di firma e la generazione dei certificati digitali (laddove richiesto), renderizzazione di immagini, verifica di documenti PDF e TIFF; l'SDK si rivolge essenzialmente allo sviluppo di applicazioni in ambito desktop e mobile, supporta quindi i principali SO (Windows e Linux per il lato desktop, Android e iOS per quello mobile) ed è distribuita nei principali linguaggi di programmazione ad alto livello (C/C++ e Java).

Faremo riferimento all'SDK provvisto per la piattaforma Windows, ultima versione: 1.18[5]; il linguaggio scelto è il C++.

### SignWare SDK

Se il SignDoc SDK contiene API destinate a coprire lo stadio finale del processo di firma (ossia la generazione e l'apposizione della firma nel documento), il SignWare SDK si occupa della fase di acquisizione della firma grafometrica e della sua eventuale verifica e validazione; integra funzioni per l'interfacciamento con i dispositivi di firma (si veda la sezione 4.1.3 per un elenco esauriente dei dispositivi compatibili), la gestione degli input da parte dell'utente che interagisce con il device esterno, la verifica dei parametri biometrici legati alla dinamica della firma, la possibilità di esportare tali dati in un formato binario proprietario, ecc.; questo kit si rivolge maggiormente all'ambito web server, tipicamente per l'integrazione di funzionalità remote di firma attraverso plugin per browser.

Anche in questo caso ci baseremo sull'SDK fornito per la piattaforma Windows, versione: 2.3.1 (ultima versione disponibile: 3.0.0[6]); il linguaggio scelto è il C.

[4] Application Programming Interface.

[5] Ultimo aggiornamento: 19 Giugno 2012.

[6] Ultimo aggiornamento: 14 Agosto 2012.

La figura 4.3 fornisce uno schema generale dei due SDK e dei relativi ambiti di applicazione. Le due interfacce sono chiaramente interoperabili e ciò favorisce la progettazione del processo di firma completo (acquisizione, apposizione e successiva verifica) in un'unica soluzione stand-alone.

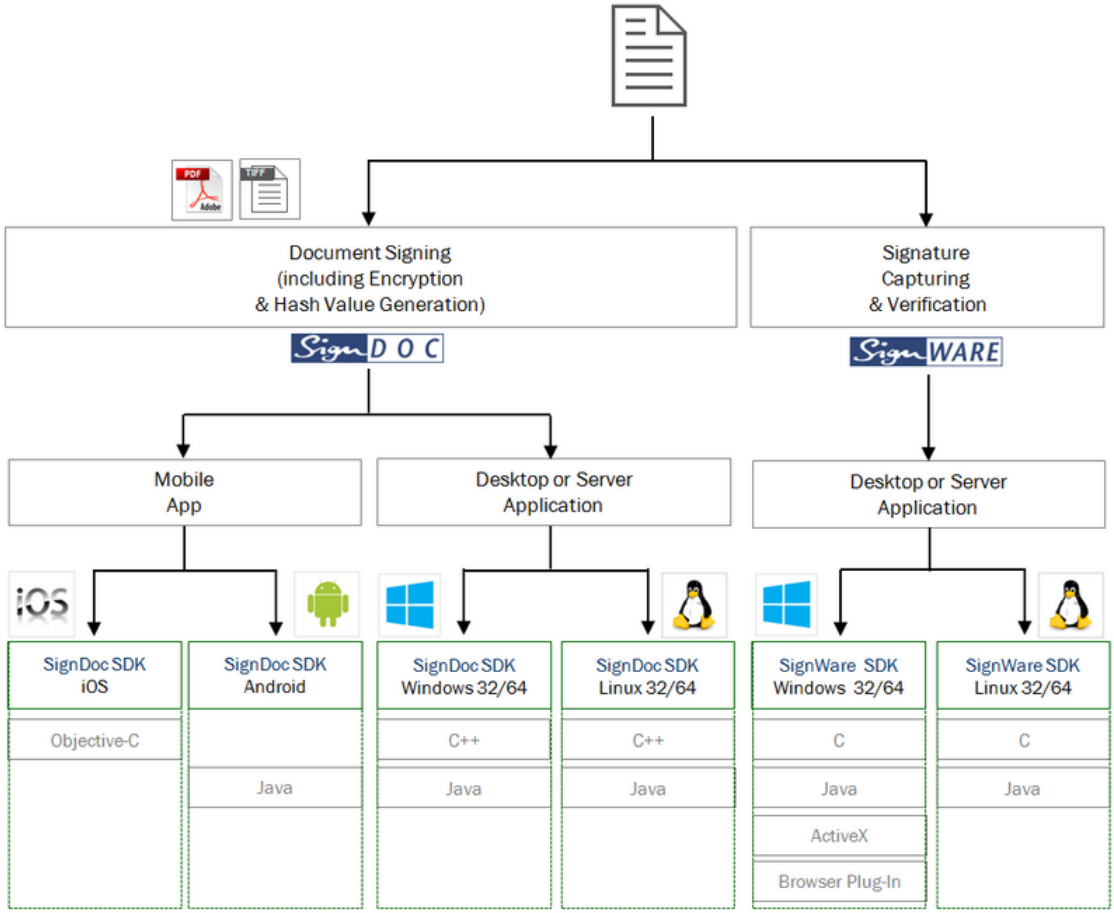


Figura 4.3. SignDoc SDK e SignWare SDK a confronto (fonte: SignDoc SDK and SignWare SDK).

### 4.1.3 Dispositivi di firma

I vari dispositivi di firma, accomunati dalla caratteristica di acquisizione ad alta precisione di signature ed estrapolazione di caratteristiche biometriche (sezione 3.3.2) dalla dinamica di firma, si diversificano in realtà per una serie di proprietà, quali la presenza o meno di un display, le caratteristiche tecniche, il costo, ecc.

Data l'ampia gamma di dispositivi compatibili con le API Softpro, è utile organizzarli secondo le diverse tipologie:

- *Pen Pad*: tablet privi di schermo LCD; il vantaggio principale di questi dispositivi risiede nel costo contenuto dovuto all'assenza del display; indicato nei casi in cui è necessario che la firma elettronica sia affiancata da una firma autografa per ragioni legali e quando l'obiettivo principale è la cattura della firma, senza ulteriori interazioni con il sistema da parte dell'utente;
- *SignPad (o Signature Pad)*: tablet progettati esplicitamente per la cattura della firma; si avvalgono di un display LCD a colori o B/N, di tipo resistivo (le dimensioni dipendono dal modello, ma si possono raggiungere gli 800 × 480 pixel di risoluzione), per la rilevazione

dei movimenti esercitati dalla penna sullo schermo; la tecnologia EMR[7] permette di rilevare soltanto i movimenti della penna e non eventuali pressioni o contatti accidentali delle dita; il dispositivo di riferimento per la nostra soluzione sarà un SignPad, in particolare un Wacom STU-520;

- *Tablet generici*: display interattivi, sistemi kiosk, tablet-PC, ecc.;
- *Dispositivi mobili*: i generici smartphone.

La figura 4.4 mostra alcuni esempi di dispositivi, suddivisi per categoria.

| Pen Pad | SignPad | Interactive Pen Display | Kiosk System | Tablet & Tablet PC |
|---|---|---|---|---|
|  *Pen Pad Wacom Mini Signature Tablet* |  *Wacom STU-520* |  *Wacom Cintiq-12* |  *Desko Tablet Kiosk* |  *Olivetti Olipad Graphos* |
|  *Wacom Bamboo One Pen* |  *Wacom STU-500* |  *Wacom PL-1600* | |  *Microsoft Surface Pro Tablet* |
|  *Wacom Intuos* |  *Wacom STU-300* |  *Wacom PL-2200* | | |

Figura 4.4. Classificazione dei dispositivi di firma, con esempi.

### Innovazioni recenti: Euronovate SA

Le possibilità di rinnovamento tecnologico che possono svilupparsi in quest'ambito e l'esigenza crescente di instaurare processi eco-sostenibili hanno portato alla nascita, nel febbraio del 2012, di Euronovate SA [18], una start-up italiana con sede operativa in Svizzera, focalizzata sulla realizzazione di processi industriali "paper free" svincolati dall'uso del cartaceo a favore dell'utilizzo integrale di documenti digitali firmati con firma elettronica, avente pieno valore legale (al pari della firma autografa). Come già trattato nella sezione 4.1.1, l'adozione di documenti nativi digitali permette la riduzione dei costi derivanti dall'uso della carta, la stampa, l'archiviazione e la ricerca manuale.

La società punta ad una re-ingegnerizzazione dei processi tradizionali di contrattualistica, con l'obiettivo di eliminare dal 70% al 90% [19] di tutta la carta gestita nelle operazioni di presa visione e firma dei contratti su carta, stipulati tra le aziende ed i loro clienti.

In questa sezione si intende affrontare una breve disamina sull'innovazione introdotta dal dispositivo attualmente impiegato dai processi Euronovate: *EN sign 10* (figura 4.5) [20]; esso si

[7] Electron Magnetic Resonance.

configura come un tablet di firma appartenente alla categoria generale dei SignPad, dotato delle seguenti caratteristiche hardware:

- display a colori LCD TFT, formato 16 : 9, dimensione diagonale: 10.1 in;
- risoluzione video: $1024 \times 600$ pixel;
- 262k colori;
- dimensioni: $263 \times 173 \times 16$ mm;
- peso: 750 g;
- chassis privo di viti (ne impedisce la manomissione, sebbene ne precluda anche la riparazione).

Di seguito invece le caratteristiche di firma:

- tecnologia EMR;
- area sensibile all'acquisizione: $222 \times 125$ mm;
- riconoscimento di 1024 livelli di pressione (10 bit);
- acquisizione di 150 campioni al secondo;
- rilevazione dei movimenti della penna fino ad una distanza di 10 mm.


Figura 4.5. EN Sign 10, dispositivo di firma di Euronovate SA (fonte: Euronovate products).

Dei cinque principali parametri di riconoscimento biometrico della firma riportati nella sezione 3.3.2, il sistema dell'EN sign 10 ne sfrutta tre: la pressione, la velocità e la posizione della penna (in termini della relativa inclinazione rispetto alla superficie); a questi va aggiunta una caratteristica innovativa, peculiare del dispositivo, ossia la capacità di rilevare i "salti in volo", di cui Alberto Guidotti, fondatore e AD della società, afferma [21]:

> [...] i cosiddetti salti in volo, i temporanei stacchi che caratterizzano il modo di firmare di tutti. È dimostrato che quando qualcuno cerca di falsificare una firma, tende a interporre un po' di tempo tra la prima e la seconda parte, tra il nome e il cognome

Questa proprietà concorre ad incrementare la sicurezza nell'associazione della firma all'identità del firmatario, consentendo di rilevare in modo più preciso in fase di verifica l'eventuale discrasia tra il template biometrico registrato e quello ottenuto, in fase di acquisizione, da un soggetto non abilitato; naturalmente, come già spiegato, la firma grafometrica in sé non costituisce firma elettronica avanzata, ma la strategia di dotare il dispositivo di caratteristiche avanzate che agevolino la fase di acquisizione (e successiva verifica) della firma contribuisce all'innalzamento del livello di efficienza del processo sviluppato.

# Capitolo 5

# Progetto: soluzione di FEA

Questo capitolo è interamente dedicato alla progettazione della nostra soluzione di firma elettronica avanzata, dall'analisi delle classi, delle funzioni e delle librerie adottate alla descrizione dei moduli, delle interfacce e delle strutture dati.

## 5.1 Premessa

Prima di procedere è necessario fare alcune considerazioni preliminari. L'ambiente di sviluppo di riferimento per l'applicazione sarà Microsoft Visual Studio 2010 Ultimate v10.0 SP1 [22]; l'applicazione utilizza componenti grafici .NET (gestiti dallo stesso framework), tuttavia la logica implementata è scritta in un linguaggio nativo (C o C++, a seconda delle esigenze di progetto e delle caratteristiche delle funzioni di libreria invocate), per questo motivo si farà uso della specifica C++/CLI[1] [23], per permettere quindi una corretta interazione tra codice *managed* (codice eseguito tramite ambiente di esecuzione CLR[2], ad esempio codice C#, VB.NET, in generale codice .NET) e *unmanaged* (codice eseguito direttamente dal processore, scritto in C e C++); all'interno dell'ambiente faremo uso del framework .NET v4.0.

La figura 5.1 mostra la pagina principale dell'IDE[3]; nella parte sinistra, scheda Esplora soluzioni, è possibile ricavare le seguenti informazioni:

- la soluzione *SoftPro_project* è composta da un solo progetto, avente lo stesso nome della soluzione;
- le cartelle *include* e *sorgenti* contengono i file principali del progetto, tra cui i file di intestazione (.h) delle librerie che compongono i due SDK già citati nella sezione 4.1.2, ossia SignDoc SDK e SignWare SDK;
- il punto di ingresso dell'applicazione è il file `SoftPro_project2.cpp`.

Alcune note di configurazione:

- il namespace del progetto è *SoftPro_project2*;
- è stata specificata un'ottimizzazione del codice da parte del compilatore di visual studio; si è scelta una *Ottimizzazione completa (/Ox)* [24], che favorisce una maggiore velocità nell'esecuzione del codice.

[1] Common Language Infrastructure.

[2] Common Language Runtime.

[3] Integrated Development Environment.

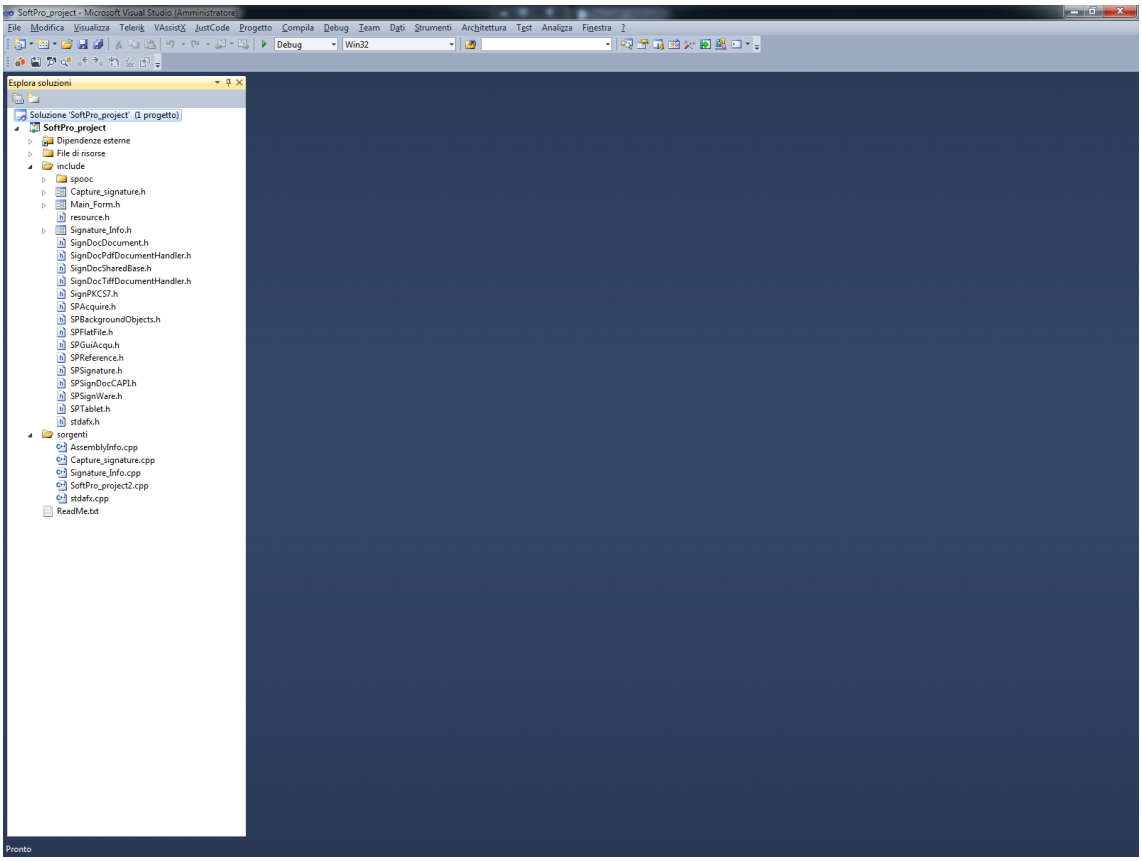


Figura 5.1. Microsoft Visual Studio 2010.

### 5.1.1 Punto di ingresso

In figura 5.2 viene riportato il codice del `main()`, contenuto nel file `SoftPro_project2.cpp`.

```
1  int main(array<System::String ^> ^args) {
2
3          Application::EnableVisualStyles();
4          Application::SetCompatibleTextRenderingDefault(false);
5
6          setlocale (LC_CTYPE, "");
7
8          Application::Run(gcnew Main_Form());
9
10         return 0;
11
12 }
```

Figura 5.2. Funzione main().

Le linee 3 e 4 attivano gli effetti visivi prima di creare i controlli, l'istruzione alla linea 6 imposta le informazioni per il "locale", che definisce il modo di interpretare ed effettuare operazioni di I/O[4]

[4]Input/Output.

prendendo in considerazione le impostazioni specifiche del linguaggio (la costante LC_CTYPE riguarda le funzioni di gestione caratteri multibyte e wide). Infine l'istruzione alla linea 8 crea la finestra principale dell'applicazione e la esegue.

### 5.1.2 Finestra principale

La figura 5.3 mostra la finestra principale, istanza della classe managed Main_Form (derivata della classe Form), punto di ingresso della nostra applicazione di FEA.

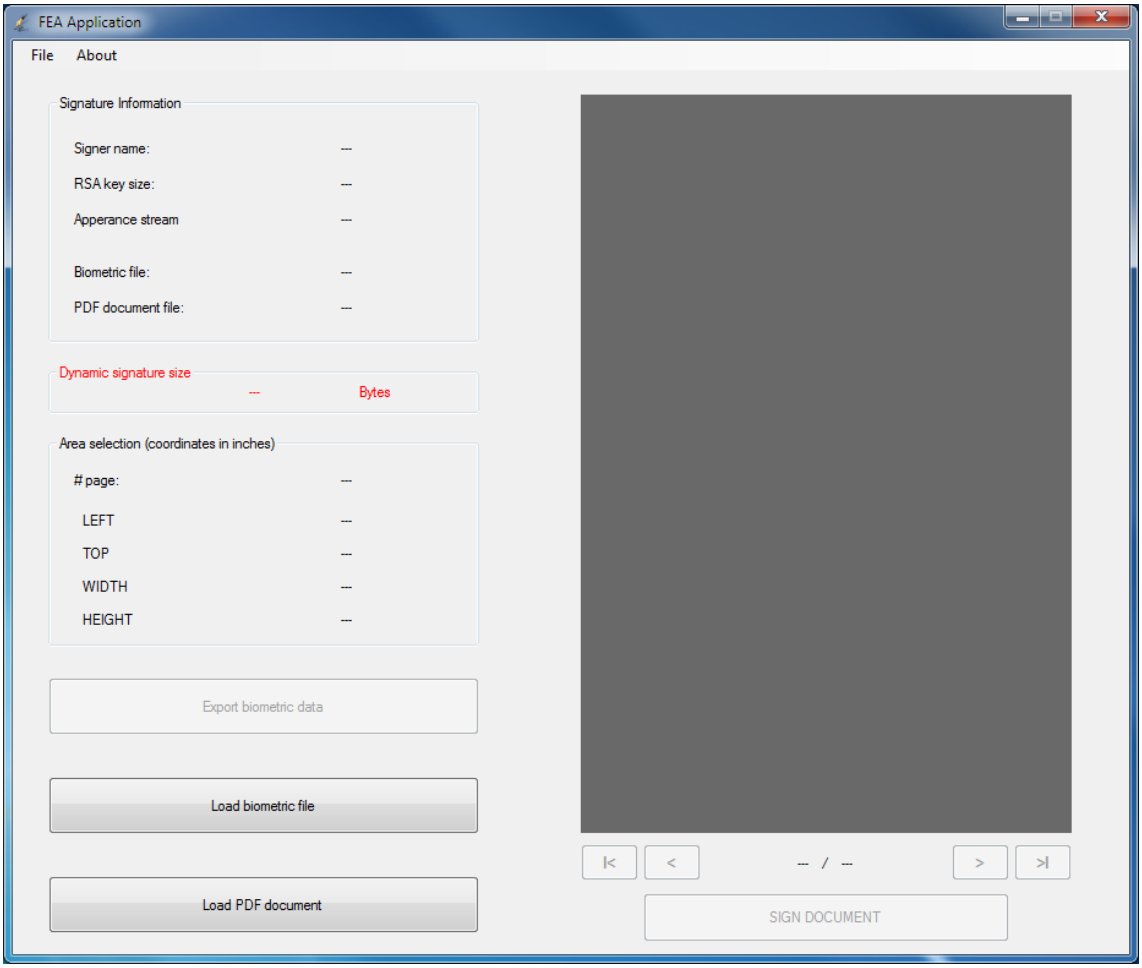


Figura 5.3. Finestra principale.

Suddivideremo l'analisi in tre macro categorie:

1. Acquisizione dei dati biometrici di firma da dispositivo tablet (sezione 5.2);
2. Inserimento parametri di configurazione di firma (sezione 5.3);
3. Generazione ed apposizione della firma su un documento in formato PDF (sezione 5.4).

L'ordine con cui verranno trattate le suddette categorie non coincide necessariamente con quello previsto dal flusso di esecuzione dell'applicazione, determinato dagli input dell'utente firmatario; nel dettaglio, le prime due procedure possono essere eseguite in un ordine arbitrario; inoltre la fase di acquisizione dei dati di firma non è obbligatoria.

## 5.2 Acquisizione dei dati biometrici

Questa fase consiste nell'acquisizione dei dati di firma grafometrica ottenuti dal processo di apposizione (da parte dell'utente, per mezzo di una penna) di una firma autografa sul dispositivo esterno (faremo riferimento nel seguito a dispositivi tablet SignPad, sezione 4.1.3 per maggiori dettagli).

Dalla finestra principale l'utente accede alla procedura attraverso il menu dei comandi, selezionando File → Capture signature, come indicato nella figura 5.4.


Figura 5.4. Selezione della funzione Capture signature dal menu dei comandi.

Viene quindi creata un'istanza della classe gestita Capture_signature (derivata della classe Form) e lanciato il costruttore (sezione 5.2.2); viene quindi mostrata a video la finestra di acquisizione firma (sezione 5.2.3).

### 5.2.1 Moduli di SignWare

La classe Capture_signature è la struttura dedicata all'acquisizione della firma grafometrica e sfrutta alcune funzioni di libreria del SignWare SDK, di cui nella figura 5.5 viene fornita una rappresentazione generale di tutti i moduli e dei collegamenti reciproci.

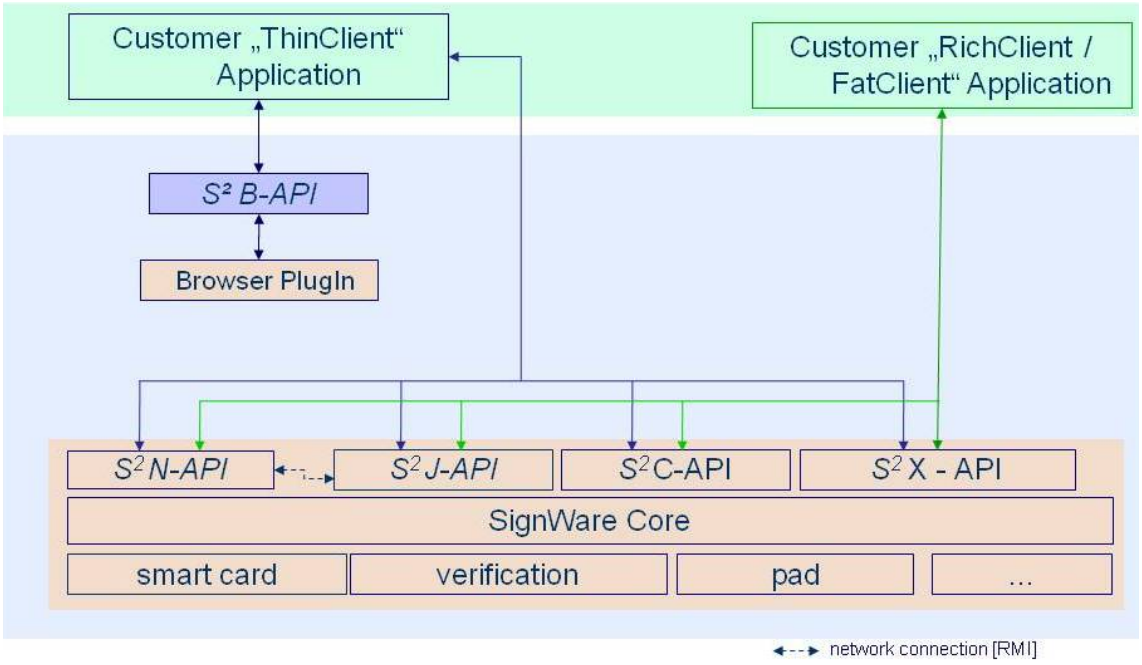


Figura 5.5. Moduli del SignWare SDK.

Il modulo funzionale ai nostri scopi è il $S^2$C-API, contenente le funzioni C di accesso al core dell'SDK. I principali header cui faremo accesso sono:

- SPGuiAcqu.h;
- SPSignature.h;

- SPFlatFile.h.

### 5.2.2 Costruttore: Capture_signature()

Il costruttore si occupa di inizializzare e configurare determinati campi della classe per la successiva connessione ed interfacciamento con il dispositivo di firma. Le sezioni seguenti analizzano nel dettaglio la logica implementativa.

#### CaptureData

Struttura C-style principale della classe, costituita da quattro campi. La sua dichiarazione e definizione nella figura 5.6.

```
1  struct CaptureData {
2
3          pSPGUIACQU_T acquire;
4
5          pSPSIGNATURE_T signature;
6
7          const char *function;
8
9          int result;
10
11 };
```

Figura 5.6. Struttura CaptureData.

Descrizione dei campi:

- acquire: variabile di tipo pSPGUIACQU_T (definito a sua volta come struct SDKGUIACQU_S* nell'header `SPSignWare.h`), rappresenta un puntatore all'oggetto usato per la cattura della firma. Tali oggetti implementano la GUI[5] per la cattura delle firme su tablet;
- signature: variabile di tipo pSPSIGNATURE_T (definito a sua volta come struct SDKSIGNATURE_S* nell'header `SPSignWare.h`), rappresenta un puntatore all'oggetto contenente la firma catturata, ossia i dati biometrici ed informazioni sul tablet utilizzato per la cattura; l'oggetto è definito da una sequenza di campioni (*tablet vector*), ciascuno dei quali è caratterizzato da:
  - coordinata $X$ del campione[6];
  - coordinata $Y$ del campione;
  - valore di pressione del campione, normalizzato al range $0 \dots 1023$, indipendentemente dal massimo valore di pressione che il tablet è in grado di percepire.
- function: puntatore al nome della funzione SignWare che dovesse fallire durante l'esecuzione del programma (restituendo un valore diverso da SP_NOERR, pari a 0);
- result: valore restituito dalla funzione SignWare che fallisce (se nessuna funzione dovesse fallire, il suo valore sarà SP_NOERR).

[5] Graphical User Interface.

[6] Coordinate-tablet.

### Costruttore

Definita la variabile statica capture_data (di tipo CaptureData), il primo passo consiste nell'inizializzazione della struttura appena descritta:

```
capture_data.acquire = NULL;
capture_data.signature = NULL;
capture_data.function = NULL;
capture_data.result = SP_NOERR;
```

Ciò che segue è una successione di invocazioni di funzioni SignWare.

```
1 int sw = SPGuiAcquCreate (&(capture_data.acquire), window_handle);
2 if (!check (&capture_data, sw, "SPGuiAcquCreate()")) {
3         // Gestione errore
4         /* ... */
5 }
```

Figura 5.7. SPGuiAcquCreate().

La funzione SPGuiAcquCreate() crea un oggetto SPGuiAcqu, rappresentato da una window nativa che riceve messaggi con ID che iniziano al valore WM_USER + 1000.
Parametri:

1. ppSPGuiAcqu [o]: doppio puntatore al nuovo oggetto SPGuiAcqu. La funzione chiamante è responsabile della deallocazione dell'oggetto creato, invocando la funzione SPGuiAcquFree();
2. hwndParent [i]: handle alla parent window.

Valori di ritorno[7]:

- SP_NOERR (0): codice relativo ad una esecuzione corretta della funzione;
- SP_PARAMERR (-1): è stato passato un parametro invalido; vedere sezione 5.2.4 per maggiori approfondimenti;
- SP_MEMERR (-6): out of memory.

```
1 sw = SPGuiAcquConnect (capture_data.acquire, SP_UNKNOWN_DRV);
2 if (!check (&capture_data, sw, "SPGuiAcquConnect()")) {
3         // Gestione errore
4         /* ... */
5         // Free all resources used by an SPGuiAcqu object.
6         SPGuiAcquFree (&(capture_data.acquire));
7         /* ... */
8 }
```

Figura 5.8. SPGuiAcquConnect().

La funzione SPGuiAcquConnect() effettua la connessione ad un tablet specificando l'ID del driver.
Parametri:

[7] Tutte le costanti sono definite nel file `SPSignWare.h`.

1. pSPGuiAcqu [i]: puntatore all'oggetto SPGuiAcqu, creato precedentemente con l'invocazione della funzione SPGuiAcquCreate();
2. iDriver [i]: l'ID del driver, passare SP_UNKNOWN_DRV (0) per riferirsi a qualsiasi driver; vedere sezione 5.2.4 per maggiori approfondimenti.

Valori di ritorno:

- SP_NOERR (0): codice relativo ad una esecuzione corretta della funzione;
- SP_PARAMERR (-1): è stato passato un parametro invalido; vedere sezione 5.2.4 per maggiori approfondimenti;
- SP_BUSYERR (-25): busy error; il tablet è in uso da un'altra applicazione;
- SP_UNSUPPORTEDERR (-5): il tablet non è supportato in questo contesto.

```
1 sw = SPGuiAcquAcquire (capture_data.acquire);
2 if (!check (&capture_data, sw, "SPGuiAcquAcquire()")) {
3         // Gestione errore
4         /* ... */
5         // Free all resources used by an SPGuiAcqu object.
6         SPGuiAcquFree (&(capture_data.acquire));
7         /* ... */
8 }
```

Figura 5.9. SPGuiAcquAcquire().

La funzione SPGuiAcquAcquire() pone il tablet in modalità *acquire*, durante la quale il dispositivo è sensibile ai movimenti della penna sulla superficie dello schermo; i tratti di firma saranno notificati alla finestra creata con la funzione SPGuiAcquCreate(), che li riprodurrà su schermo (si veda il capitolo 6 per una simulazione completa del processo di firma).

La funzione, impostata la suddetta modalità, ritorna immediatamente. Gli eventuali cambiamenti di stato del tablet sono segnalati da funzioni di callback come:

- SPAcquireSetTimeout;
- SPAcquireRegisterRect;
- SPAcquireRegisterRect2;
- SPAcquireSetButtonListener.

Parametro:

1. pSPGuiAcqu [i]: puntatore all'oggetto SPGuiAcqu, creato precedentemente con l'invocazione della funzione SPGuiAcquCreate();

Valori di ritorno:

- SP_NOERR (0): codice relativo ad una esecuzione corretta della funzione;
- SP_PARAMERR (-1): è stato passato un parametro invalido; vedere sezione 5.2.4 per maggiori approfondimenti;

- SP_BUSYERR (-25): busy error; il tablet è in uso da un'altra applicazione;

La funzione check() incontrata nei vari listati verifica ad ogni occorrenza il valore di ritorno; qualora esso sia diverso da quello atteso (SP_NOERR) assegna ai campi function e result della variabile capture_data il nome della funzione che ha generato l'errore e il codice dell'errore, rispettivamente. Segue una gestione dell'eccezione da parte della funzione chiamante.

In tale contesto la funzione SPGuiAcquFree(), ove presente, rilascia le risorse allocate (in particolare l'oggetto SPGuiAcqu).

Questo conclude l'analisi del costruttore.

### 5.2.3 Finestra di acquisizione firma

Dichiarata ed inizializzata l'istanza della classe Capture_signature(), viene invocato il metodo pubblico ShowDialog(), che visualizza il form come finestra di dialogo modale (figura 5.10). Essa

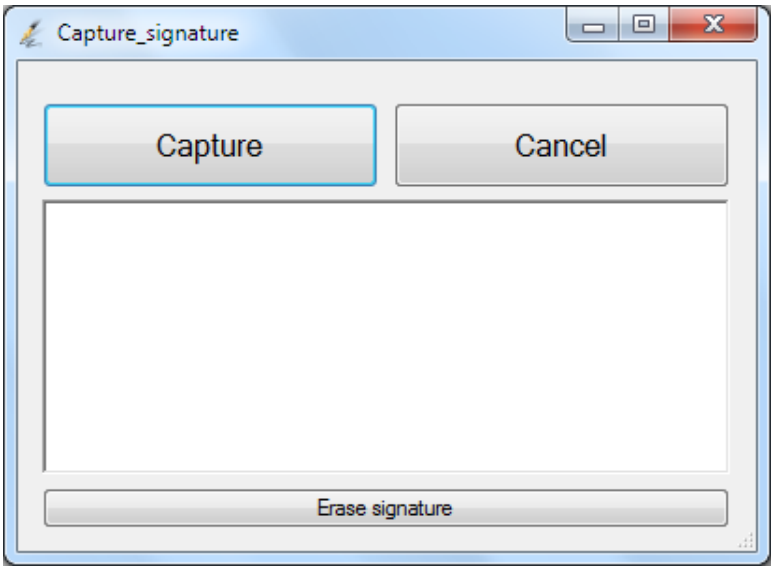


Figura 5.10. Finestra di acquisizione firma grafometrica.

presenta tre pulsanti: le sezioni seguenti analizzano il comportamento dell'applicazione al click su ciascuno di essi.

#### Capture

Con il click sul pulsante Capture l'utente fa richiesta di acquisizione della firma apposta sul tablet. Segue l'invocazione in una serie di funzioni di libreria. La funzione principale è la SPSignature-CreateFromGuiAcqu() (figura 5.11), che ottiene la firma apposta in modalità *acquire* del tablet. Parametri:

1. ppSignature [o]: doppio puntatore all'oggetto SPSignature; tale oggetto conterrà i dati biometrici (se ne è già discusso nella sezione 5.2.2);
2. pSPGuiAcqu [i]: puntatore all'oggetto SPGuiAcqu.

Valori di ritorno:

- SP_NOERR (0): codice relativo ad una esecuzione corretta della funzione;

```
1  int sw = SPSignatureCreateFromGuiAcqu (&(capture_data.signature),
       capture_data.acquire);
2  if (check (&capture_data, sw, "SPSignatureCreateFromGuiAcqu()"))
3          sw = SPGuiAcquAcquireDone (capture_data.acquire, IDOK);
4  else
5          sw = SPGuiAcquAcquireDone (capture_data.acquire, IDCANCEL);
6  if (!check (&capture_data, sw, "SPGuiAcquAcquireDone()")) {
7          // Gestione errore
8          /* ... */
9  }
10 SPGuiAcquFree (&(capture_data.acquire));
```

Figura 5.11. SPSignatureCreateFromGuiAcqu().

- SP_PARAMERR (-1): è stato passato un parametro invalido; vedere sezione 5.2.4 per maggiori approfondimenti;
- SP_MEMERR (-6): out of memory.

Indipendentemente dall'esito dell'esecuzione, la funzione invocata successivamente nel blocco if-else, SPGuiAcquAcquireDone() (linee 3 e 5 del listato in figura 5.11), termina la modalità *acquire*. Parametri:

1. pSPGuiAcqu [i]: puntatore all'oggetto SPGuiAcqu;
2. iResult [i]: due possibili valori:
   - SP_IDOK (1): memorizza definitivamente la firma nell'oggetto SPSignature;
   - SP_IDCANCEL (2): ignora la firma.

A questo punto, se la cattura ha avuto successo, l'oggetto SPGuiAcqu viene rilasciato (linea 10). La fase successiva consiste nell'esportazione dei dati biometrici in un formato di file di tipo *flat*[8], che consenta, nel caso di specie, l'accesso ai dati biometrici per mezzo di un array di byte (char). La funzione SPFlatFileCreateFromSignature() crea un oggetto in formato SP_FF_SOFTPRO (0)[9] a partire da un oggetto SPSignature precedentemente inizializzato (vedi figura 5.12).
Parametri:

1. ppbFlatFile [o]: doppio puntatore all'oggetto che conterrà i dati biometrici in formato proprietario; la funzione chiamante è responsabile della sua deallocazione chiamando la funzione SPFlatFileFree() (alla linea 11);
2. piFlatFileLength [o]: puntatore alla variabile che conterrà la dimensione (in byte) dell'oggetto inizializzato dalla stessa funzione;
3. pSignature [i]: puntatore all'oggetto SPSignature.

Valori di ritorno:

- SP_NOERR (0): codice relativo ad una esecuzione corretta della funzione;

[8] Vengono chiamati *flat file* tutti quei file il cui contenuto non presenta logiche strutturali.

[9] Formato di firma biometrica sicuro, proprietario della Softpro.

```
1  SPUCHAR *bio_ptr = NULL;
2  SPINT32 bio_size = 0;
3  sw = SPFlatFileCreateFromSignature (&bio_ptr, &bio_size,
       capture_data.signature);
4  if (sw != SP_NOERR) {
5          // Gestione errore
6          /* ... */
7  }
8  /* Utilizzo dei dati biometrici puntati da bio_ptr (unsigned char*) */
9  /* ... */
10 SPSignatureFree (&(capture_data.signature));
11 SPFlatFileFree (&bio_ptr);
```

Figura 5.12. SPFlatFileCreateFromSignature().

- SP_PARAMERR (-1): è stato passato un parametro invalido; vedere sezione 5.2.4 per maggiori approfondimenti;
- SP_MEMERR (-6): out of memory.

La funzione SPSignatureFree(), alla linea 10, dealloca quindi l'oggetto SPSignature, non più necessario.

#### Cancel

Il click sul pulsante Cancel determina la chiusura della finestra modale ed il ritorno a quella principale (vedi figura 5.3). Il delegato associato a tale evento si compone delle seguenti istruzioni:

```
1  SPGuiAcquAcquireDone (capture_data.acquire, IDCANCEL);
2  SPGuiAcquFree (&(capture_data.acquire));
```

#### Erase signature

Il click sul pulsante Erase signature invalida il contenuto della window nativa rappresentato dall'oggetto SPGuiAcqu creato nel costruttore, consentendo all'utente di ripetere il processo di tracciamento della firma sullo schermo del tablet. Le istruzioni del delegato:

```
1  SPGuiAcquAcquireDone (capture_data.acquire, IDCANCEL);
2  int sw;
3  sw = SPGuiAcquConnect (capture_data.acquire, SP_UNKNOWN_DRV);
4  sw = SPGuiAcquAcquire (capture_data.acquire);
```

### 5.2.4 Costanti

Questa sezione riporta le costanti e gli ID dei driver principali citati precedentemente, dedicando a ciascuno di essi una descrizione aggiuntiva.

La ricezione di un valore di ritorno SP_PARAMERR (-1) indica il passaggio di un parametro invalido ad una funzione, ad esempio:

- un puntatore nullo, laddove non previsto;

- un valore numerico out-of-range;
- un puntatore che non punta ad oggetti del tipo corretto;
- un oggetto il cui stato non supporta l'operazione richiesta;
- un buffer con dimensione troppo piccola;
- uno specifico file che non può essere aperto.

Quello che segue è invece l'elenco degli ID dei driver definiti in SignWare:

- SP_UNKNOWN_DRV (0): identificatore per qualsiasi driver di tablet;
- SP_WINTAB_DRV (1): driver Wintab;
- SP_PADCOM_DRV (2): driver MobiNetix;
- SP_NATIVE_DRV (3): driver nativo Softpro;
- SP_TCP_DRV (4): driver remoto Softpro;
- SP_TABLETSERVER_DRV (5): driver del TabletServer Softpro.

## 5.3 Inserimento parametri di configurazione

In questa fase l'utente interagisce con una finestra modale per fornire in input una serie di valori che determineranno alcuni parametri di configurazione nella fase conclusiva del processo di firma. Dalla finestra principale l'utente accede alla procedura attraverso il menu dei comandi, selezionando File → Signature Info, come indicato nella figura 5.13.

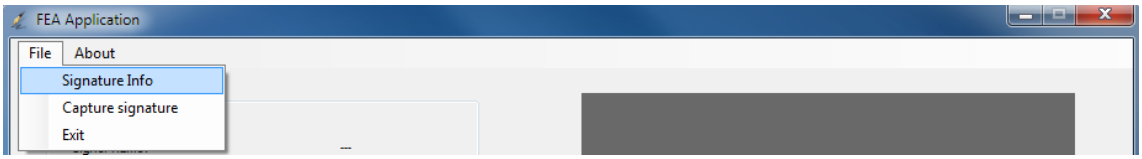


Figura 5.13. Selezione della funzione Signature Info dal menu dei comandi.

Viene quindi creata un'istanza della classe gestita Signature_Info (derivata della classe Form) e mostrata a video la finestra modale (figura 5.14). La finestra si compone di tre controlli (nell'ordine: textbox, checkbox, combobox), attraverso i quali il programma acquisisce i seguenti tre parametri di firma (obbligatori, tra parentesi il loro tipo):

- *Signer name* (char*): il valore che l'utente inserisce nella textbox costituirà il nome del firmatario del documento; esso comporrà anche il campo *Common Name* (vedi 3.2.5) del certificato self signed creato durante l'operazione di firma;
- *Appearance stream* (bool): attraverso la checkbox l'utente decide se rendere visibile il proprio nome (quello inserito nel controllo precedente) all'interno del riquadro che conterrà l'immagine renderizzata della firma biometrica (si veda la sezione 6.5 per un esempio che mostri la differenza tra le due scelte in termini di resa grafica);
- *Key size* (int): l'utente ha facoltà di scegliere tra tre diversi valori: 1024, 2048, 4096; con questo controllo l'utente decide la dimensione (in bit) della coppia di chiavi RSA utilizzate per la generazione della firma digitale (vedi sezione 5.4); la dimensione della chiave influenzerà in modo determinante il tempo computazionale di creazione della firma: si è già parlato di questo aspetto nella sezione 3.2.1, sul tema della crittografia a chiave pubblica.

La sezione successiva tratterà della fase conclusiva dell'intero processo, ovvero la generazione ed apposizione della firma sul documento.

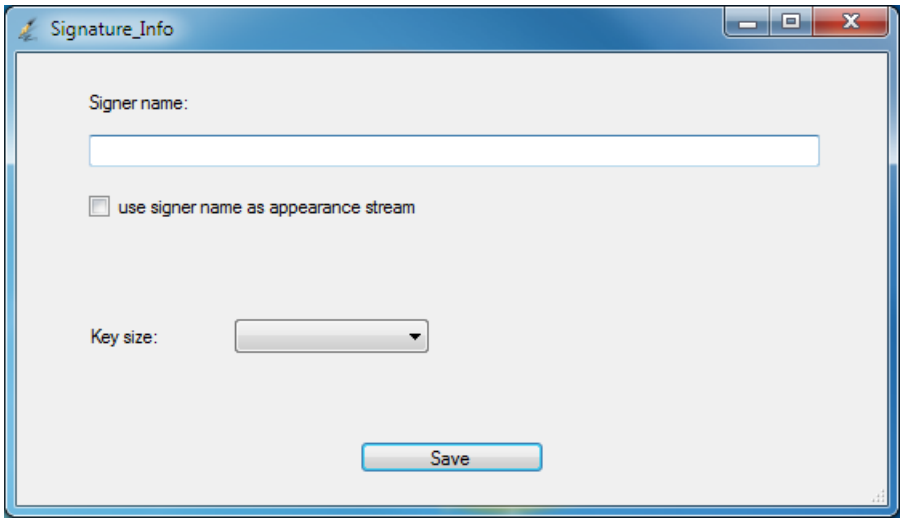


Figura 5.14. Finestra di acquisizione valori in input.

## 5.4 Generazione della firma

Prima che si possa procedere con l'analisi conclusiva del processo di firma è necessario che l'utente abbia selezionato il documento PDF da firmare: ciò viene realizzato premendo il pulsante Load PDF document della finestra principale (vedi figura 5.3); l'evento scatena la visualizzazione del pdf scelto nel controllo corrispondente (rettangolo scuro nella stessa finestra); si tratta di un controllo .NET proprietario, dedicato alla gestione ed elaborazione di documenti PDF [25].

Mediante tale controllo l'utente ha la facoltà di scegliere in quale pagina (ed in quale regione all'interno della pagina) apporre la propria firma grafometrica; se la scelta della pagina non è obbligatoria (di default viene scelta la prima), lo è invece la selezione dell'area rettangolare in cui sarà mostrata l'immagine renderizzata della firma (vedi figure 5.15 e 5.16).


Figura 5.15. Documento PDF visualizzato nel controllo GdPicture .NET.


Figura 5.16. Selezione dell'area su cui apporre la firma.

La posizione dell'area rettangolare è definita da un sistema di coordinate (in pollici) avente origine nell'angolo in alto a sinistra della pagina visualizzata (si veda sezione 5.4.3 per una spiegazione dettagliata).

Terminate le operazioni precedenti, l'utente può completare il processo premendo il pulsante SIGN DOCUMENT della finestra principale. Il delegato associato a tale evento invoca la funzione privata sign() della classe Main_form.

### 5.4.1 Funzione sign()

Le attività principali della funzione sign() riguardano la configurazione di alcuni parametri necessari alla creazione della firma digitale (se ne esporranno i dettagli nelle successive sezioni), quindi l'apposizione della firma sul documento. Essa farà riferimento a funzioni di libreria C++ del SignDoc SDK, contenute nelle seguenti tre classi:

- SignDocDocumentLoader (`SignDocDocument.h`): permette la creazione di oggetti SignDocDocumentLoader presso cui registrare gli handler di documenti da firmare;
- SignDocDocument (`SignDocDocument.h`): una interfaccia per l'istanziazione di oggetti SignDocDocument, ciascuno dei quali rappresenta un documento;
- SignDocPdfDocumentHandler (`SignDocPdfDocumentHandler.h`): rappresenta oggetti handler di documenti PDF; in figura 5.17 è mostrato il diagramma di ereditarietà.

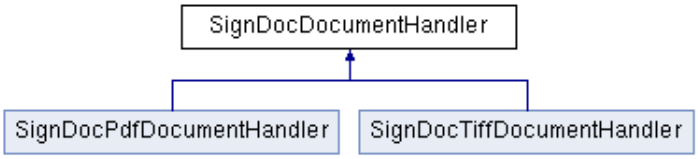


Figura 5.17. Diagramma di ereditarietà della classe SignDocPdfDocumentHandler.

### 5.4.2 Registrazione del documento

La prima fase consiste nella registrazione del documento presso l'handler appropriato; in figura 5.18 il listato completo.

```
1 SignDocDocumentLoader* loader = new SignDocDocumentLoader();
2
3 loader->registerDocumentHandler (new SignDocPdfDocumentHandler);
4
5 SignDocDocument *doc = loader->loadFromFile (enc_native, document_path, true);
6 if (doc == NULL) {
7         // Gestione errore
8 }
```

Figura 5.18. Registrazione del documento.

La linea 1 inizializza l'oggetto SignDocDocumentLoader, quindi l'istruzione successiva registra un handler (di tipo SignDocPdfDocumentHandler); la funzione loadFromFile() della linea 5 si occupa di caricare il documento da firmare e restituirne un puntatore (SignDocDocument*).
Parametri:

1. aEncoding [i]: la codifica della stringa passata come secondo parametro; vedere la sezione 5.4.9 per maggiori dettagli;
2. aPath [i]: path del documento da firmare (ricavato precedentemente dalla gestione dell'evento "click" sul pulsante Load PDF document);
3. aWritable [i]: booleano che stabilisce se il documento è aperto per la scrittura (come nel caso in esame, per cui firmare il documento sovrascriverà il documento stesso).

### 5.4.3 Inserimento campo firma: funzione addSignatureField()

La funzione descritta in questa sezione ha il compito di costruire un oggetto di tipo SignDocField (classe dichiarata nel file `SignDocDocument.h`), che rappresenta un campo di firma, ed inizializzarlo ai valori ottenuti nella fase preliminare di composizione del rettangolo nella pagina del documento.

Come già anticipato, le coordinate dell'area rettangolare sono espresse in pollici e hanno origine nel punto in alto a sinistra della pagina; il rettangolo di selezione è definito dalle seguenti proprietà (vedi figura 5.19):

- Left: posizione sinistra dell'area selezionata;
- Top: posizione superiore dell'area selezionata;
- Width: larghezza dell'area selezionata;
- Height: altezza dell'area selezionata.

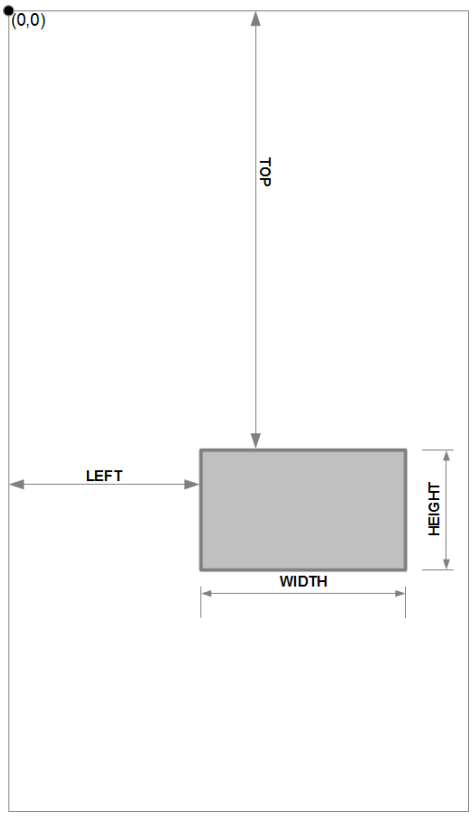


Figura 5.19. Sistema di coordinate del rettangolo di selezione nel controllo GdPicture .NET.

Il SignDoc SDK adotta tuttavia un diverso criterio: l'origine del sistema di coordinate è nell'angolo in basso a sinistra della pagina e l'unità di misura adottata è il **punto tipografico** (pt), che equivale

ad 1/72 di pollice. La funzione addSignatureField() si occupa del corretto passaggio da un sistema all'altro applicando opportuni fattori di conversione, quindi aggiunge al documento il campo rappresentato dall'oggetto SignDocField (con la funzione addField()), dopo averne configurato:

- il nome, con la funzione setName();
- il tipo, con la funzione setType(); possibili valori:
  - t_unknown: tipo sconosciuto;
  - t_pushbutton: pulsante;
  - t_check_box: casella di controllo;
  - t_radio_button: pulsante di opzione;
  - t_text: campo testo;
  - t_choice: list box, combo box, ecc.;
  - t_signature_digsig: Digital signature field (*Adobe DigSig*), quello scelto per il progetto;
  - t_signature_signdoc: Digital signature field (campo tradizionale SignDoc).
- le coordinate, con le funzioni setLeft(), setRight(), setBottom(), setTop().

### 5.4.4 Parametri

L'ultima fase, che prelude alla generazione ed apposizione della firma (realizzata infine con la funzione addSignature()), consiste nella definizione e configurazione di alcuni **parametri di firma**. I parametri disponibili dipendono dal tipo di documento e dal tipo del campo di firma creato in precedenza (vedi sezione 5.4.3); la funzione addSignature() successiva potrebbe fallire se i parametri settati non sono validi o presentano conflitti.

```
1 SignDocSignatureParameters *params = NULL;
2 SignDocDocument::ReturnCode rc;
3 rc = doc->createSignatureParameters (enc_native, fieldName, "", params);
```

Figura 5.20. Creazione parametri di firma

La funzione createSignatureParameters() crea un'istanza della classe SignDocSignatureParameters (file `SignDocDocument.h`), necessaria per porre la firma nell'omonimo campo; la funzione chiamante (in questo caso sign()) è responsabile della distruzione dell'oggetto.
Parametri:

- aEncoding [in]: la codifica adottata per il secondo parametro; vedere sezione 5.4.9 per maggiori dettagli;
- aFieldName [in]: il nome del campo di firma (sezione 5.4.3);
- aProfile [in]: il nome del profilo (ASCII); alcuni tipi di documenti e campi di firma supportano differenti set di parametri di default. Il profilo di default ("") è supportato da tutti i campi di firma;
- aOutput [out]: un puntatore all'oggetto istanza di SignDocSignatureParameters qui creato.

Le sezioni seguenti esaminano nel dettaglio i principali parametri adottati in questa soluzione; distinguiamo i parametri in tre categorie:

- Parametri interi (sezione 5.4.5);
- Parametri blob (sezione 5.4.6);
- Parametri stringa (sezione 5.4.7).

### 5.4.5 Parametri interi

#### GenerateKeyPair

```
pr = params->setInteger ("GenerateKeyPair", key_size);
```

Genera una coppia di chiavi RSA per il certificato self signed. Con il secondo parametro si specifica la dimensione delle chiavi (da 1024 a 4096, ma multiplo di 8); si noti che tale valore è già stato determinato in fase di inserimento dei parametri di configurazione (sezione 5.3).

Quando viene generato un certificato self signed, la chiave privata può essere generata o impostando questo parametro o impostando il parametro blob "CertificatePrivateKey" (qui non considerato).

#### Method

```
pr = params->setInteger ("Method",
    SignDocSignatureParameters::m_digsig_pkcs7_detached);
```

Definisce il metodo di firma. Se non viene specificato ne verrà scelto uno di default. Sono disponibili:

- m_signdoc: metodo tradizionale SignDoc (metodo a blocchi);
- m_digsig_pkcs1: PDF DigSig PKCS #1;
- m_digsig_pkcs7_detached: PDF DigSig detached PKCS #7;
- m_digsig_pkcs7_sha1: PDF DigSig PKCS #7 con SHA-1;
- m_hash: la firma è semplicemente un hash.

#### RenderSignature

```
pr = params->setInteger ("RenderSignature",
    SignDocSignatureParameters::rsf_gray);
```

Specifica se e come la firma biometrica (recepita con il parametro blob "BiometricData", vedere sezione 5.4.6) debba essere renderizzata per l'immagine di firma. Possibili valori (definiti nell'enumerazione SignDocSignatureParameters::RenderSignatureFlags, mutuamente esclusivi):

- rsf_bw: immagine in B/N (bianco e nero);
- rsf_gray: rappresentazione in toni di grigio.

Se il valore passato è 0 la firma non sarà renderizzata (come si è già visto nella sezione 5.2, SignWare SDK è richiesto per acquisire e quindi renderizzare la firma). Se non è stata impostata nessuna immagine (tramite il parametro blob "Image", qui non considerato, ma se presente sostituisce questo parametro intero), il campo di firma può o no mostrare un'immagine calcolata dai dati biometrici, in base al tipo di documento e al tipo del campo di firma. Il valore di default è 0.

#### BiometricEncryption

```
pr = params->setInteger ("BiometricEncryption",
    SignDocSignatureParameters::be_fixed);
```

Specifica come i dati biometrici debbano essere cifrati (i dati biometrici sono quelli specificati con il parametro blob "BiometricData"); se questo parametro non è settato i dati biometrici non saranno incorporati nella firma. Possibili valori (definiti nell'enumerazione SignDocSignatureParameters::BiometricEncryption):

- be_rsa: utilizzo di una chiave simmetrica random, cifrata con una chiave pubblica RSA. Deve essere impostato il parametro blob "BiometricKey" (con cui indicare la chiave RSA (be_rsa) o la chiave AES (be_binary) con cui cifrare la chiave simmetrica) oppure il parametro stringa "BiometricKeyPath" (con cui specificare il path del file contenente la chiave pubblica RSA in formato PKCS #1);
- be_fixed: utilizzo di una chiave simmetrica fissa, non cifrata;
- be_binary: chiave binaria a 256 bit; deve essere impostato il parametro "BiometricKey";
- be_passphrase: la chiave simmetrica verrà generata a partire da una passphrase (calcolata su 256 bit); deve essere settato il parametro stringa "BiometricPassphrase";
- be_dont_store: i dati biometrici non saranno incorporati nel documento; usare questa opzione se si intende utilizzare i dati biometrici solo per generare un'immagine di firma.

### 5.4.6 Parametri blob

#### BiometricData

```
pr = params->setBlob ("BiometricData", biometric_signature,
    biometric_signature_size);
```

Con questo parametro si specificano i dati biometrici da includere nel documento (opportunamente cifrati secondo le modalità viste in precedenza). I dati devono essere in formato SignDoc o in formato SignWare (ricavato con la funzione SPFlatFileCreateFromSignature(), come già visto in 5.2.3) e saranno utilizzati per renderizzare l'immagine della firma se il parametro intero "RenderSignature" è diverso da 0 (a meno che un'immagine di firma non sia stata specificata con il parametro blob "Image").

Il secondo parametro è un puntatore al primo ottetto della struttura contenente i dati, il terzo indica la dimensione del blob (il numero di ottetti).

### 5.4.7 Parametri stringa

#### CommonName

```
pr = params->setString (enc_native, "CommonName", signer_name);
```

Imposta il campo *common name* (sezione 3.2.5) per il certificato self signed. Quando viene generato un certificato self signed tale campo deve essere obbligatoriamente presente.
Parametri:

1. aEncoding [i]: la codifica adottata per il terzo parametro (vedi 5.4.9);
2. aName [i]: il nome del parametro;
3. aValue [i]: il valore del parametro.

**Signer**

```
pr = params->setString (enc_native, "Signer", signer_name);
```

Il nome del firmatario: questo è il nome che verrà memorizzato nella firma digitale. Se non impostato, il nome sarà preso dal certificato (campo CN, Common Name). Per i campi firma di tipo *DigSig* (come quello utilizzato in questo contesto) il nome del firmatario può essere usato per l'appearance stream (sezione 5.3) dei documenti PDF. Il valore di default è vuoto.

**Font**

```
pr = params->setString (enc_native, "Font", "Helvetica");
```

Il nome del font. Per i campi DigSig questo parametro definisce il font da usarsi per l'appearance stream dei documenti PDF.

### 5.4.8 Firma del documento

```
rc = doc->addSignature (params);
```

La funzione addSignature(), considerate le configurazioni dei parametri sopra analizzate, firma il documento. Se il parametro stringa "OutputPath" è impostato, il documento sarà memorizzato in un nuovo file il cui path è specificato da quel parametro. Se il parametro stringa "TemporaryDirectory" è impostato (e non lo è "OutputPath"), il documento sarà memorizzato in un nuovo file temporaneo. In entrambi i casi il file originario non verrà modificato (comunque sarà cancellato se è un file temporaneo, cioè se "TemporaryDirectory" è stato usato). Se né "OutputPath" né "TemporaryDirectory" sono stati impostati il documento sarà sovrascritto (è questo il caso).

Al documento è stata apposta una **firma digitale**; tale firma è calcolata sul documento, insieme ai dati biometrici ivi contenuti, cifrati con la chiave simmetrica indicata precedentemente dal parametro intero *BiometricEncryption*; al documento è associato anche il certificato self signed e quindi la chiave pubblica necessaria per la verifica dell'integrità del documento stesso.

I dati biometrici sono stati utilizzati per la renderizzazione dell'immagine di firma e possono eventualmente essere considerati come elemento probatorio in una perizia calligrafica (svolta da esperti calligrafici che hanno accesso alla chiave con cui decifrare i dati e su autorizzazione delle parti coinvolte); ulteriori considerazioni in quest'ambito sono destinate al capitolo conclusivo della tesi (capitolo 7).

### 5.4.9 Costanti ed enumerazioni

Codifiche adottate nel SignDoc SDK (definite dall'enumerazione de::softpro::doc::Encoding):

- enc_native: Windows "ANSI" per un sistema Windows, LC_CTYPE per un sistema Linux;
- enc_utf_8: UTF-8;
- enc_latin_1: ISO 8859-1.

# Capitolo 6

# Processo e risultati sperimentali

Analizzata la soluzione applicativa di FEA in tutte le sue principali componenti nel precedente capitolo, procediamo ad illustrare un tipico processo di firma attraverso una esecuzione dell'applicazione sviluppata.

Al termine del processo verrà svolta un'analisi dei risultati ottenuti.

## 6.1 Processo

Il flusso di esecuzione del processo ad alto livello ricalca quello mostrato in figura 6.1.

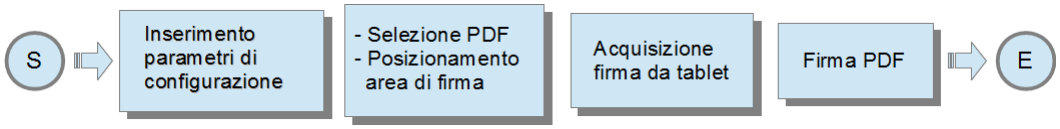


Figura 6.1. Flusso di esecuzione del processo.

Avviata l'esecuzione del programma, l'utente può interagire con i pulsanti e le voci di menu; in figura 5.3 è mostrata la finestra principale.

## 6.2 Inserimento parametri di configurazione

Dalla main window l'utente firmatario seleziona File → Signature Info ed inserisce i seguenti input:

- *Signer name*: Mario Rossi;
- *Appearance stream*: impostato a true (checkbox spuntata);
- *Key size*: 1024.

Il risultato è mostrato in figura 6.2.

Prima che l'utente prema il pulsante Save i campi relativi al nome del firmatario e alla dimensione della chiave devono essere stati compilati, in quanto obbligatori (la finestra avvisa l'utente di ciò con un MessageBox). Al ritorno dalla finestra modale lo stato di quella principale è in figura 6.3. Possiamo notare come i dati inseriti dall'utente siano adesso visualizzati nel riquadro *Signature Information* (evidenziati dall'ellisse). È possibile quindi procedere con l'operazione successiva.

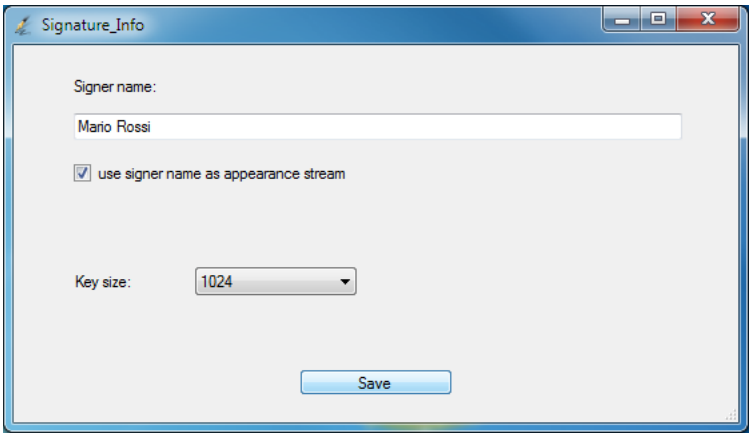


Figura 6.2. Finestra Signature_Info con i valori inseriti dall'utente.

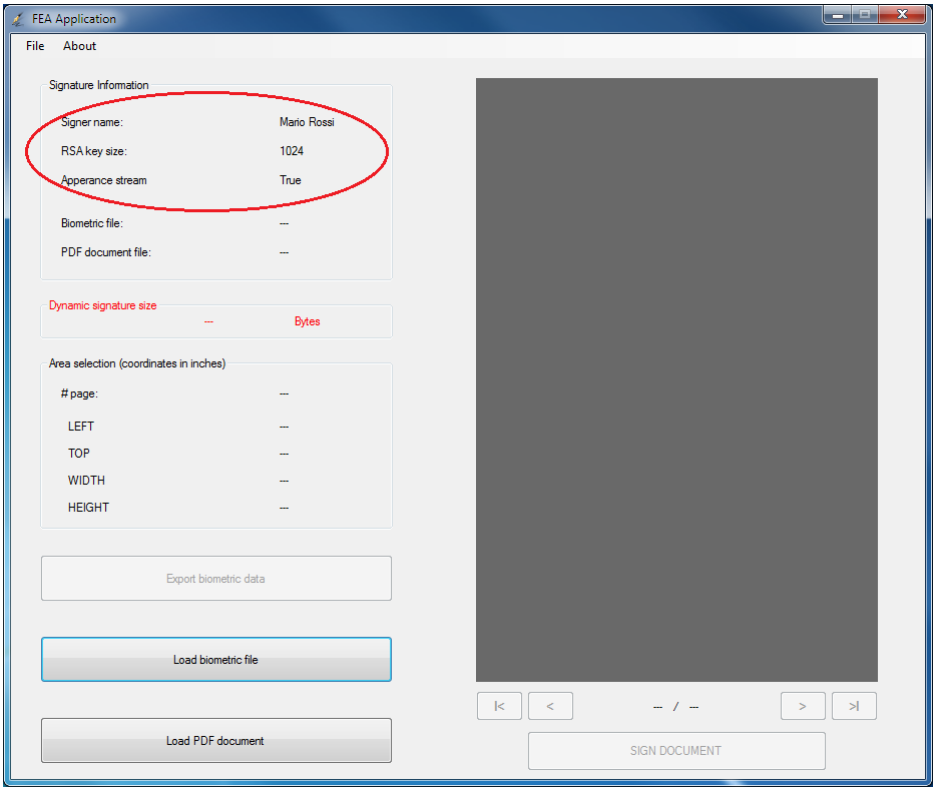


Figura 6.3. Finestra principale al ritorno dalla finestra Signature_Info.

## 6.3 Selezione PDF e campo firma

Alla pressione del pulsante Load PDF document viene aperta una finestra modale mediante la quale l'utente può selezionare il documento PDF da firmare. Visualizzato il documento nella regione della finestra dedicata a tale funzione e individuata la pagina desiderata, con il click destro del mouse sul controllo GdPicture si può attivare la modalità *Area Selection* per il disegno dell'area di firma. Nelle figure 6.4 e 6.5 viene mostrato il percorso di accesso a tale modalità e la scelta della posizione del campo di firma, rispettivamente.
In figura 6.6, invece, lo stato della finestra principale ad operazioni completate.

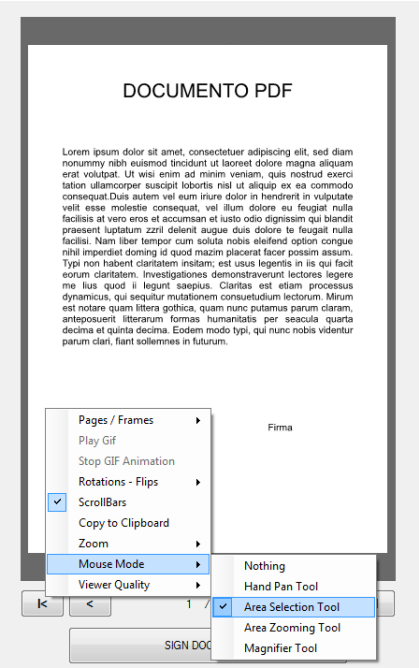


Figura 6.4. Modalità Area Selection Tool.

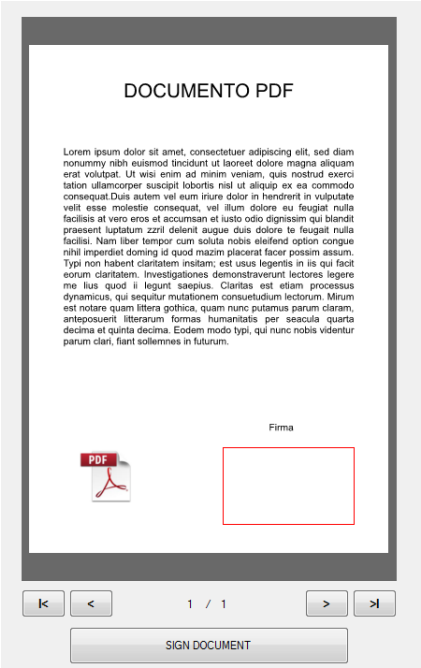


Figura 6.5. Selezione dell'area.

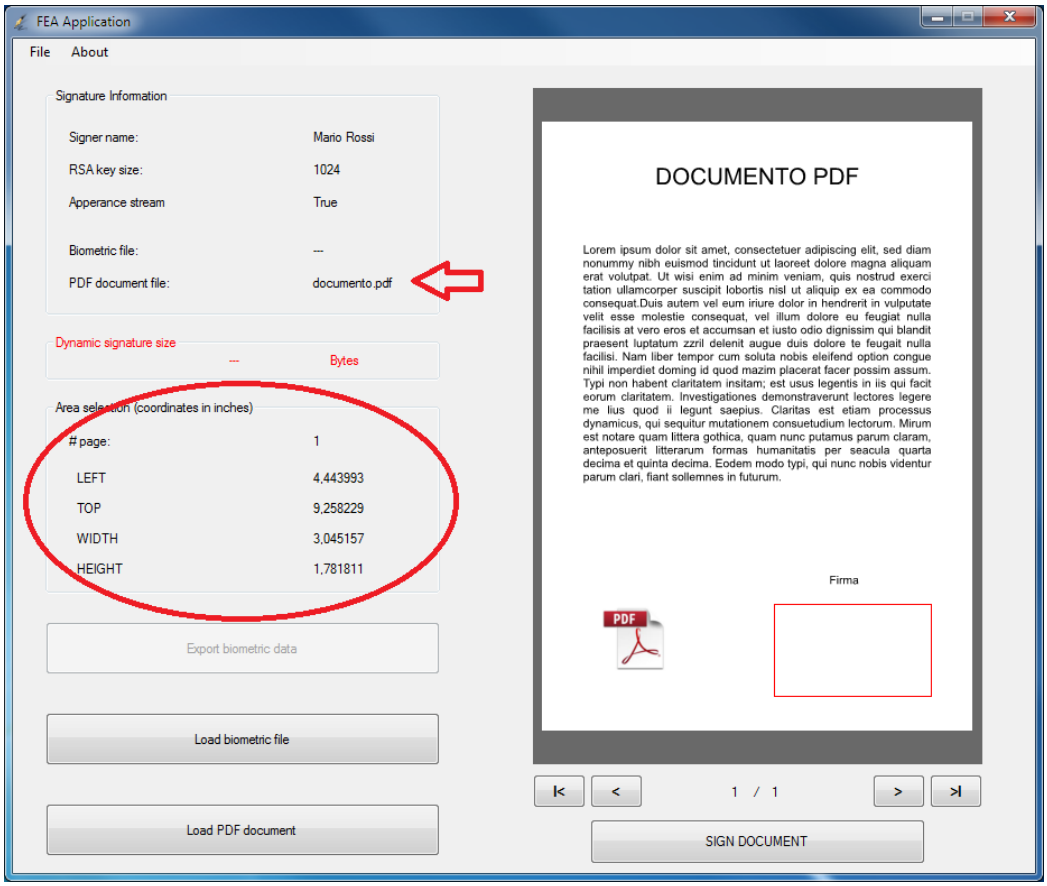


Figura 6.6. Finestra principale dopo il caricamento del documento PDF.

Come si evince dall'ultima figura, nel riquadro *Area selection* sono presenti le seguenti informazioni:

- il numero della pagina in cui è posto il campo di firma, nel caso in esame il valore è 1;
- le coordinate (in pollici) del riquadro: left, top, width, height.

All'interno del riquadro *Signature Information* è comparso anche il nome del documento appena caricato: `document.pdf`.

## 6.4 Acquisizione firma da tablet

Dalla main window l'utente seleziona File → Capture signature per accedere alla finestra di acquisizione firma. Il controllo passa quindi al dispositivo esterno (un Wacom STU-520, si veda la figura 4.4) che riproduce su schermo i movimenti esercitati dall'utente tramite la penna; grazie al cosiddetto "ink effect" l'effetto grafico sul tablet e sulla finestra di acquisizione ricorda quello di una classica firma su carta (incentivando la *user experience*). Il risultato è evidenziato dalle figure 6.7 e 6.8.

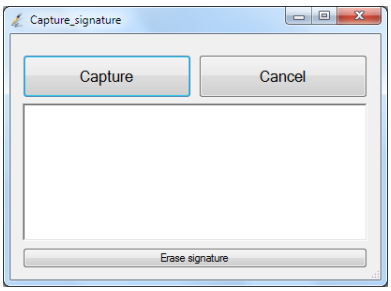


Figura 6.7. Finestra di acquisizione prima della firma.


Figura 6.8. Finestra di acquisizione durante la firma.

Alla pressione del pulsante Capture il controllo torna alla finestra principale, adesso aggiornata con nuove informazioni (figura 6.9).

Osserviamo come i dati biometrici siano stati acquisiti correttamente dal dispositivo (non si è verificato nessun errore) e di essi venga indicata, nel riquadro *Dynamic signature size*, la dimensione complessiva in byte (958 nel caso di specie). L'utente può dunque procedere con l'ultima fase del processo.

## 6.5 Firma PDF

Il click sul pulsante SIGN DOCUMENT scatena l'ultimo evento legato a questo processo, ovvero l'apposizione della firma al documento. La conclusione dell'operazione viene sancita da un MessageBox, come indicato in figura 6.10.
Il documento risulta essere quindi firmato digitalmente. Per ragioni di comparazione, nelle figure 6.11 e 6.12 viene indicata la dimensione del documento prima e dopo l'apposizione della firma.
Verifichiamo la presenza della firma aprendo il file con un visualizzatore standard di documenti PDF[1]; se il programma scelto lo consente, è anche possibile verificare la validità della firma.

Osserviamo la presenza del nome del firmatario nel riquadro di firma: come si è già visto nella sezione 6.2, l'utente ha impostato a true la proprietà dell'*Appearance stream*. Le figure 6.13 e 6.14 mostrano la differenza, in termini grafici, tra la scelta di inserire e non inserire il nome come appearance stream.

[1] Si è scelto il software *PDF-XChange Viewer* di Tracker Software Products Ltd.

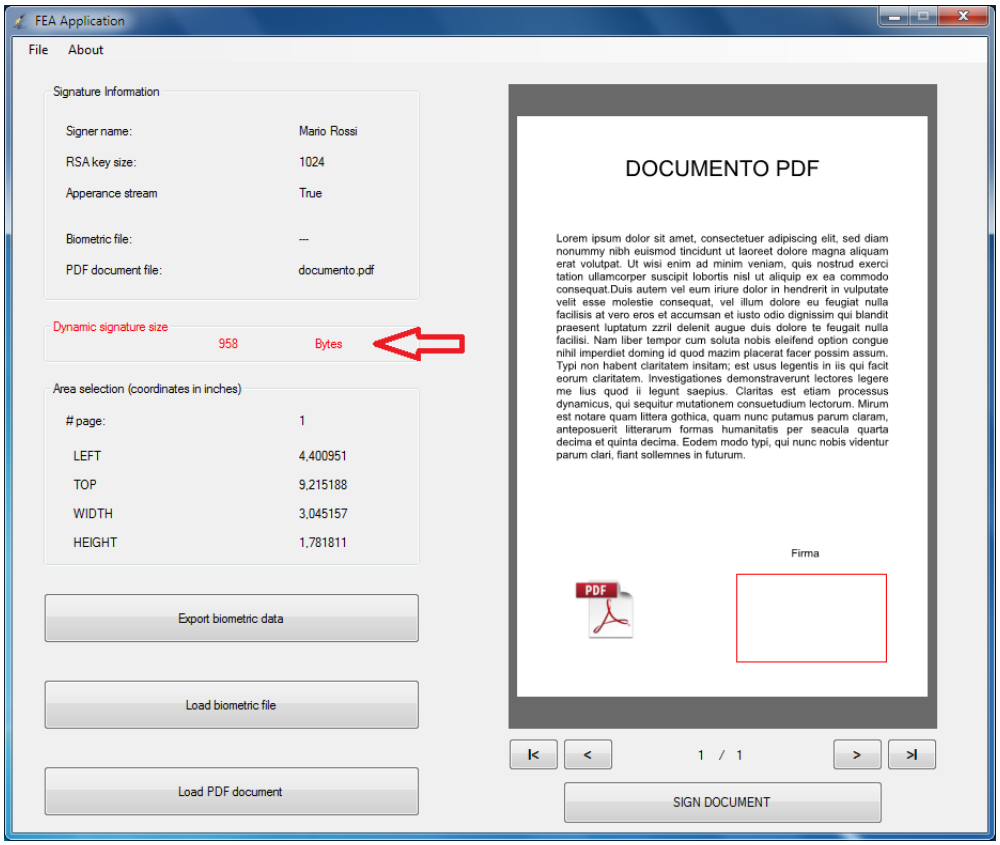


Figura 6.9. Finestra principale dopo l'acquisizione dei dati di firma.

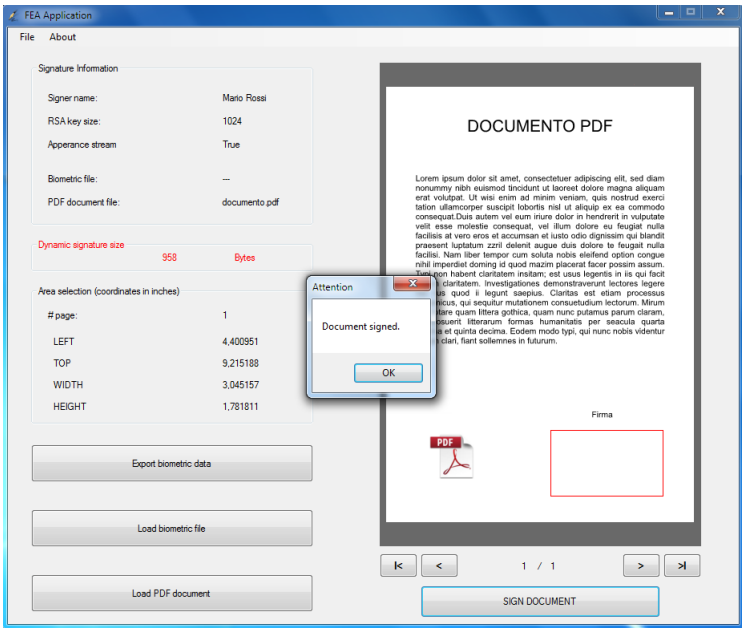


Figura 6.10. Finestra principale al termine del processo.

All'interno del documento, facendo click sul campo di firma è possibile recuperare le informazioni associate al certificato, come evidenziato in figura 6.15.
Occorre precisare che il certificato self signed generato è considerato non attendibile, in quanto non

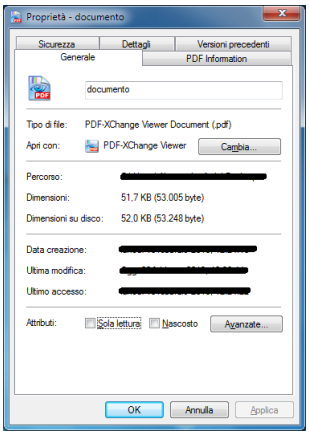


Figura 6.11. Dimensione del file non firmato.

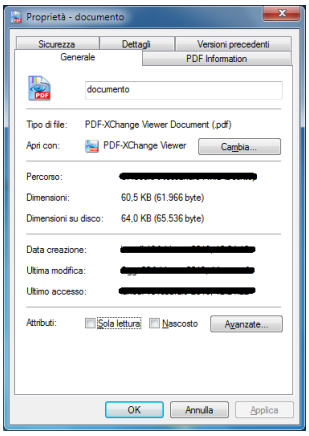


Figura 6.12. Dimensione del file dopo la firma.


Figura 6.13. Appearance stream: true.


Figura 6.14. Appearance stream: false.

presente nell'archivio delle Autorità di certificazione radice attendibili; per alcuni visualizzatori PDF (come Adobe Reader [26]) questo costituisce una condizione sufficiente per considerare non valida una firma.

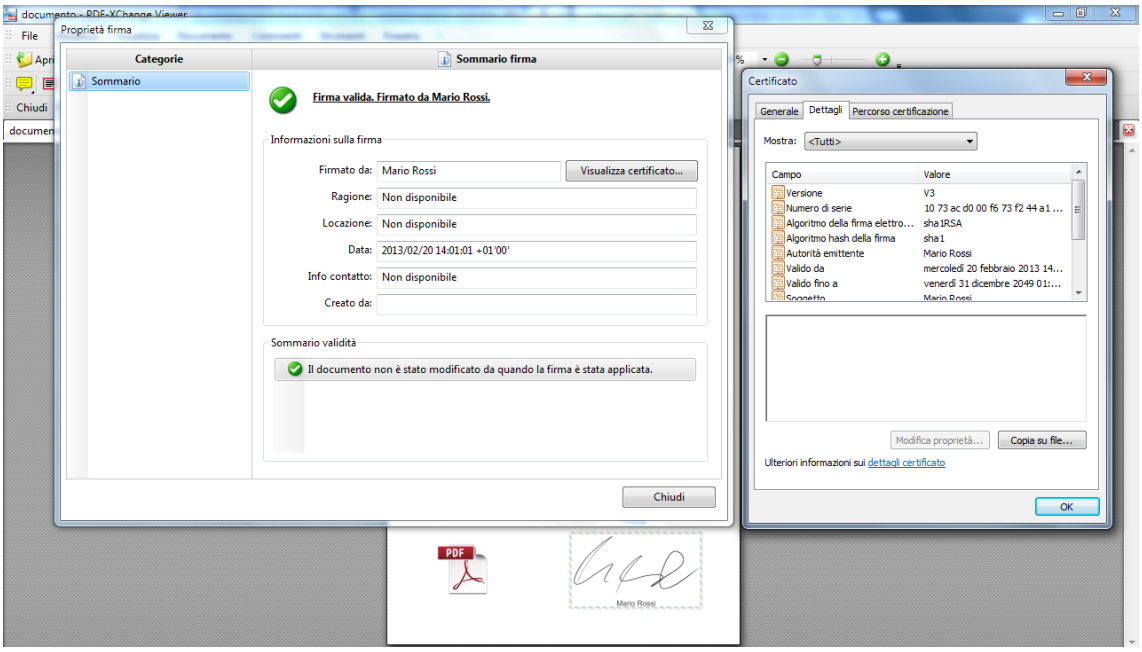


Figura 6.15. Firma digitale e certificato associato.

## 6.6 Profilatura prestazioni

Questa sezione è dedicata all'analisi dei risultati ottenuti da due sessioni di profilatura dell'applicazione, svolta dall'ambiente Visual Studio 2010; la tipologia di profilatura scelta è quella del **Campionamento CPU**, che esegue il monitoraggio del processore durante l'esecuzione dell'applicazione.

Entrambe le sessioni verranno avviate al lancio del programma e analizzeranno, per tutta la durata dell'esecuzione, il carico sulla CPU da parte di ciascuna funzione; le due sessioni si distinguono esclusivamente per gli input passati dall'utente nella finestra *Signature_Info*, nel primo caso infatti i valori sono:

1. Signer name: Mario Rossi;
2. Appearance stream: true;
3. Key size: **1024**.

Nel secondo, invece:

1. Signer name: Mario Rossi;
2. Appearance stream: true;
3. Key size: **4096**.

### 6.6.1 Prima sessione

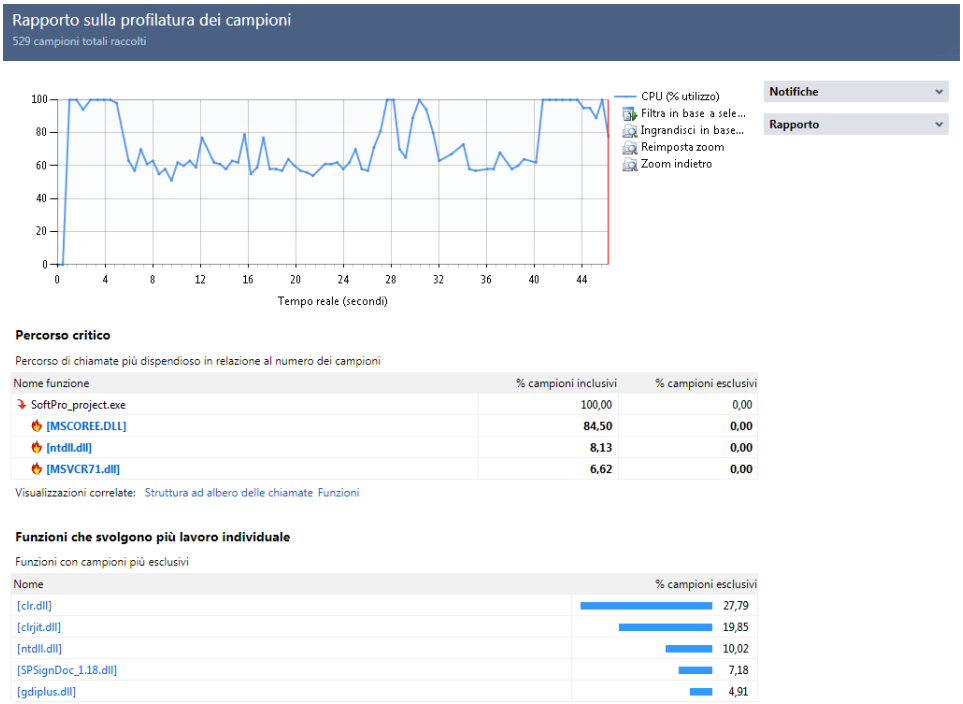


Figura 6.16. Profilatura dell'applicazione con chiavi a 1024 bit.

Osserviamo come le funzioni di firma, contenute in `SPSignDoc_1.18.dll`, occupino solo il quarto posto nell'elenco delle funzioni che svolgono più lavoro individuale (si veda l'omonima scheda nella figura), con il 7,18% di campioni esclusivi. La maggior parte del tempo è dedicata all'invocazione di funzioni del CLR, per l'interazione tra moduli gestiti e non gestiti (27,79%) durante l'esecuzione.

### 6.6.2 Seconda sessione

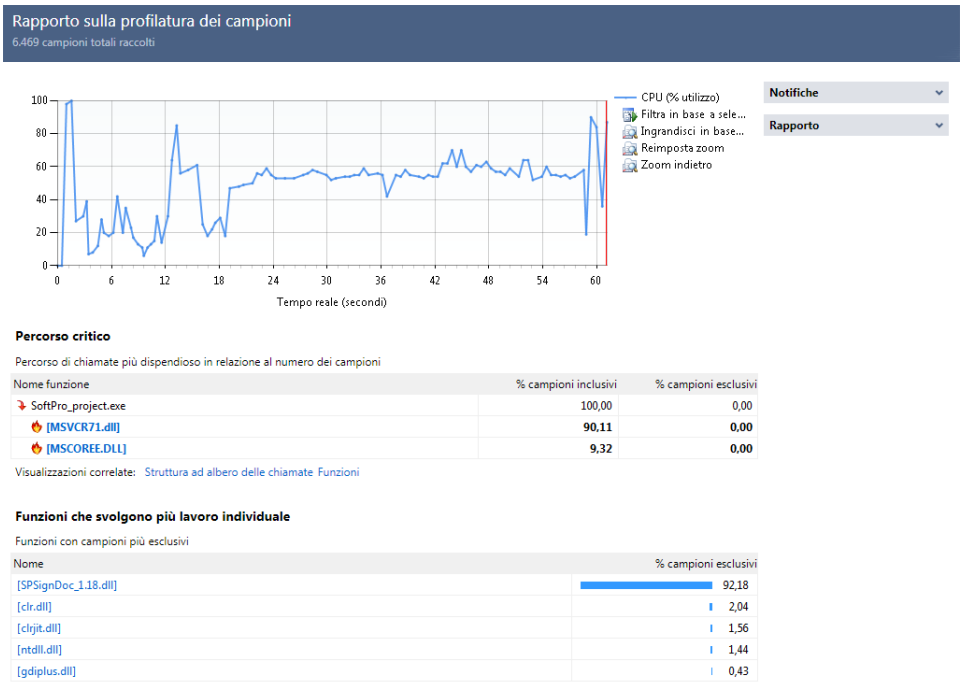


Figura 6.17. Profilatura dell'applicazione con chiavi a 4096 bit.

In questo caso le funzioni di firma occupano la maggior parte del tempo di processore (92,18%): ciò è dovuto quasi esclusivamente alla dimensione elevata delle chiavi RSA (4096 bit), che, come già trattato nella sezione 3.2.1, implicano un elevato carico computazionale nella generazione della firma.

# Capitolo 7

# Considerazioni finali e conclusioni

Esaminata nel dettaglio l'architettura funzionale della soluzione di firma elettronica avanzata sviluppata nel capitolo 5 e affrontato lo studio di un tipico processo di firma nel capitolo 6, è utile a questo punto soffermarsi su alcune considerazioni inerenti il ruolo della biometria nei casi sin qui trattati, che solleva alcune questioni legate a tematiche di privacy e sicurezza non ancora discusse. Nelle sezioni a seguire si intende focalizzare l'attenzione su aspetti integrativi della soluzione, nell'ottica di una sua realizzazione in un progetto reale.

## 7.1 Trasferimento dei dati biometrici

La soluzione presentata implementa una comunicazione in chiaro tra il tablet Wacom (figura 4.4) e l'applicazione; i dati biometrici associati alla dinamica di firma vengono dunque forniti dal dispositivo senza cifratura (sebbene comunque la libreria SignDoc li gestisca tramite un formato proprietario con presunte caratteristiche di sicurezza, vedi sezione 5.2.3); nel contesto di una implementazione per uso reale, è essenziale che il dialogo avvenga in modo cifrato, al fine di evitare intercettazioni della comunicazione e problemi di sicurezza derivanti da attacchi di tipo man-in-the-middle. I prodotti di firma disponibili in commercio offrono tipicamente soluzioni di cifratura *embedded* nel dispositivo stesso; le dichiarazioni e le specifiche tecniche riportate dal produttore del dispositivo di firma adottato non offrono indicazioni in tal senso [27].

## 7.2 Master key: gestione e protezione

Si è più volte accennato alla *master key* ed al suo ruolo nell'ambito della firma elettronica avanzata: trattasi della chiave simmetrica adottata per la cifratura dei dati biometrici, quindi quella adoperata per decifrare ed accedere alle caratteristiche di firma proprie di un firmatario (la decifrazione e l'analisi dei dati avviene tipicamente ad opera di periti grafologi che effettuano le verifiche dei parametri calligrafici di firma in sede di contenzioso legale); in quanto componente sensibile, la master key deve essere conservata e protetta in un ambiente sicuro; come già trattato nella sezione 3.3.3, una tipica gestione prevede il suo immagazzinamento in HSM simili a quelli utilizzati per le firme digitali (in genere integrato nell'elettronica dello stesso tablet).

La soluzione presentata ha fatto uso di una master key generata "al volo" (con il parametro intero BiometricEncryption, sezione 5.4.5), per l'inclusione di dati di firma cifrati all'interno del documento scelto: si tratta di un espediente facilmente realizzabile in un progetto locale, ma se applicato ad un caso reale presenta rischi per la sicurezza dei dati biometrici (chiave accessibile a terzi); altre soluzioni (come quelle previste da Softpro) prevedono l'inclusione della stessa master key all'interno del documento firmato, cifrata con la chiave pubblica della coppia di chiavi RSA associate al certificato self signed (alcuni parametri interi consentono questa procedura).

## 7.3 Trattamento dei dati personali

Un tema fortemente legato alla privacy di un utente è quello della realizzazione di banche dati che memorizzino le informazioni biometriche di ciascun individuo, elemento fondante nella costituzione di un modello organizzativo che sfrutti i dati a disposizione per condurre una verifica dell'identità del sottoscrittore [28]. Come già ampiamente discusso nella sezione 3.3.1, l'utilizzo della biometria nel campo delle firme prevede che ad una fase di acquisizione iniziale delle caratteristiche proprie della persona segua, in occasione di ogni ulteriore sottoscrizione, un confronto tra i dati già disponibili e quelli correnti, al fine di un corretto riconoscimento del firmatario. Tipicamente, in fase di registrazione, la verifica dell'identità è supportata da una fase di identificazione fisica (ad esempio tramite un documento di identità).

Evidenziamo in questo caso la criticità di sicurezza data dalla necessità di accedere ad un data center remoto in modo cifrato, onde evitare intercettazioni dei dati di firma; la soluzione qui costruita può essere estesa in modo tale da tenere in considerazione questi aspetti.

## 7.4 Criticità del dato biometrico

Le criticità associate all'uso della biometria nell'ambito delle firme elettroniche hanno origine nella natura stessa della biometrica di firma: il limite principale è dato dalla ovvia instabilità nel tempo del campione biometrico, che può determinare importanti variazioni sull'esito dei confronti tra i template in fase di verifica e causare una falsa accettazione o un falso rigetto (si rimanda alla sezione 3.3.2); una soluzione tecnologica può consistere nell'aggiornamento periodico del template registrato, in modo da garantire una certa validità dei dati nelle verifiche successive.

## 7.5 Conclusioni

L'intento prefissato nella redazione di questo elaborato è stato quello di fornire anzitutto una visione chiara, completa ed approfondita sulla normativa della firma elettronica, ed in particolare su quella della firma elettronica avanzata, strumento che, complice la continua e costante evoluzione tecnologica che ne garantisce un'affidabilità crescente nel tempo, si caratterizza ad oggi come principale componente nel processo di digitalizzazione, amministrazione e conservazione a lungo termine dei documenti digitali.

Basandosi sul principio del *technology-neutral*, le firme elettroniche avanzate sono state configurate come elemento fondante di processi di firma (svincolati dall'utilizzo di tecnologie stabilite a priori) che trovassero ampia applicabilità in vari ambiti (da quello amministrativo, realizzando la conservazione sostituiva con la firma digitale a quello bancario, mediante l'impiego delle tecnologie biometriche).

Proprio l'utilizzo della biometrica di firma, unita alle caratteristiche indicate in precedenza, ha posto le basi per lo sviluppo di una soluzione applicativa di firma elettronica avanzata che, a partire dall'interazione dell'utente con un dispositivo di firma, realizzasse l'apposizione di una firma ad un documento digitale.

La soluzione oggetto di questa tesi si configura come progetto pilota, orientato a mostrare i componenti fondamentali che governano un tipico processo di firma, ma senza pretese in termini di sicurezza effettiva, se adoperata in un contesto pratico (si vedano ad esempio le sezioni precedenti all'interno di questo capitolo); essa si presta tuttavia ad eventuali modifiche (sia dal punto di vista architetturale che implementativo) che ne migliorino l'usabilità e la sua integrabilità in casi reali.

# Bibliografia


[1] M.Nastri, F.Rolleri, "La dematerializzazione e la conservazione a lungo termine dei documenti informatici", Commissione Informatica del Consiglio Nazionale del Notariato, Roma (Italia), September 25-26, 2008, pp. 1-10, http://www.notariato.it/export/sites/default/it/primo-piano/congressi-convegni/convegno-sicurezza-giuridica-pdf/Nastri_Relazione.pdf

[2] P.Ridolfi, "Quadro normativo" nel libro "Firma elettronica: tecniche, norme, applicazioni" a cura di P.Ridolfi, F.Angeli, 2003, pp. 177-181, ISBN 88-464-4178-8

[3] Le nuove frontiere del documento informatico e della firma elettronica: dalla firma digitale attraverso quella grafometrica fino alla "mobile signature", http://www.studiolegalelisi.it/notizia.php?titolo_mod=413

[4] Il documento informatico, http://www.futurestorage.it/news-archiviazione/15-news/52-il-documento-informatico

[5] P.Ridolfi, "Tipi di firma" nel libro "Firma elettronica: tecniche, norme, applicazioni" a cura di P.Ridolfi, F.Angeli, 2003, pp. 96-97, ISBN 88-464-4178-8

[6] G.Finocchiaro, "Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale", Contratto e Impresa, No. 2, March-April 2011, pp. 495-504, ISSN 1123-5055

[7] C.Bodini, "Dematerializzazione e conservazione digitale dei documenti", Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili, December 15, 2011, pp. VII-X, http://www.commercialisti.it/Portal/Documenti/Dettaglio.aspx?id=7bd9bd2a-8c1d-4fc4-9eec-9e6a5e1bea18

[8] P.Ridolfi, "Quadro normativo" nel libro "Firma elettronica: tecniche, norme, applicazioni" a cura di P.Ridolfi, F.Angeli, 2003, p. 68, ISBN 88-464-4178-8

[9] P.Ridolfi, "Quadro normativo" nel libro "Firma elettronica: tecniche, norme, applicazioni" a cura di P.Ridolfi, F.Angeli, 2003, pp. 54-57, ISBN 88-464-4178-8

[10] What is a hash function?, http://www.rsa.com/rsalabs/node.asp?id=2176

[11] P.Ridolfi, "Quadro normativo" nel libro "Firma elettronica: tecniche, norme, applicazioni" a cura di P.Ridolfi, F.Angeli, 2003, pp. 88-94, ISBN 88-464-4178-8

[12] C.Manganelli, "Linee guida per l'impiego delle tecnologie biometriche nelle pubbliche amministrazioni", i Quaderni del CNIPA, No. 9, November 2004, pp. 31-33

[13] C.Manganelli, "Linee guida per l'impiego delle tecnologie biometriche nelle pubbliche amministrazioni", i Quaderni del CNIPA, No. 9, November 2004, pp. 42-45

[14] Softpro GmbH, https://www.softpro.de/en/

[15] Softpro as world's leading company for signature management, http://www.softpro.de/en/company/awards-certificates-recognitions-acknowledgements.aspx

[16] Softpro regulations and laws on Electronic Signatures, http://www.softpro.de/en/academy/electronic-signatures-regulations-laws-bills.aspx

[17] Joerg Lenz, "Taking Signatures seriously - Combining Biometric and Digital Signatures", Proceedings of Conference ISSE, Berlin (Germany), October 06, 2010, p. 323, DOI 10.1016/S0969-4765(10)70040-0

[18] Euronovate SA, http://www.euronovate.com/bonair/EN/index.php

[19] Euronovate SA mission, http://www.euronovate.com/bonair/EN/mission.php

[20] Euronovate SA EN Sign 10, http://www.euronovate.com/bonair/EN/products.php

[21] Data Manager Online, intervista ad Alberto Guidotti, fondatore e AD di Euronovate SA, http://www.datamanager.it/rivista/firma-digitale/una-firma-fatta-di-bit
[22] Microsoft Visual Studio, MSDN (Microsoft Developer Network) page, http://msdn.microsoft.com/en-US/vstudio
[23] C++/CLI, language specification, http://en.wikipedia.org/wiki/C%2B%2B/CLI
[24] /Ox (Full Optimization), http://msdn.microsoft.com/en-us/library/59a3b321(v=vs.80).aspx
[25] GdPicture .NET, Document Imaging and Image Processing SDK for .NET & ActiveX, http://www.gdpicture.com/
[26] Adobe Systems Inc. web site, http://www.adobe.com/it/
[27] Wacom signature solutions, http://signature.wacom.eu/
[28] G. Manca, "Il decalogo della firma grafometrica", Information Security, No. 8, January-February 2012, pp. 53-59, ISSN 2037-5611