La firma grafometrica: le applicazioni concrete.

Giovanni MANCA

27 maggio 2016 (Procedamus – Salerno)

Argomenti - 1

- **Le firme biometriche non grafometriche: aspetti tecnici e soluzioni tecnologiche.**
- **Gli obblighi in capo ai soggetti erogatori delle soluzioni di firma elettronica avanzata.**
- **I doveri di informazione nei confronti del firmatario.**

Argomenti – 2

- **L’obbligo di preventiva accettazione della soluzione da parte del firmatario.**
- **I limiti d’uso e le coperture assicurative.**
- **Le applicazioni operative nei diversi settori (assicurativo, bancario, finanziario, PPAA, ecc.).**

LE FIRME BIOMETRICHE NON GRAFOMETRICHE: ASPETTI TECNICI E SOLUZIONI TECNOLOGICHE.

Scenari d’uso della non grafometrica

- La maggior parte delle applicazioni sono iniziate con l’utilizzo della firma biometrica non grafometrica.
- Si è partiti storicamente con i grandi hotel, l’autonoleggio, la logistica e i pagamenti elettronici.
- Viene raccolto solo il dato grafico che è rappresentato dalle coordinate X e Y sul sensore.
- In qualche apparato si firma direttamente con il dito.
- In qualche applicazione sembra essere rilevato anche il dato pressorio del tratto grafico.

La non grafometrica e la Privacy

- **Rimane presente il tema del trattamento del dato personale.**
- **I dati raccolti sono facenti parte della biometria comportamentale.**
- **In alcuni scenari il dato può essere analizzato da un perito forense come se fosse impresso su carta.**
- **L'informativa sul trattamento è meno «evidente» e forse nemmeno c'è.**
- **La firma viene apposta non si sa su che cosa e non si sa come verrà trattata.**
- **Eppure i dati nel sistema ci sono…**

Non grafometrica: tecnologia

- **Tablet grafici tradizionali in genere senza sensibilità pressoria.**
- **Software in genere non identificabile dall'utente.**
- **In molti scenari viene usato l'iPAD che ha un sensore capacitivo che non è in grado di rilevare la pressione.**
- **La diffusione di iPAD lo sta rendendo estremamente appetibile anche per la non grafometrica.**
- **Esistono tecnologie avanzate e sofisticate per il riconoscimento «online» delle firme non grafometriche.**

La firma grafometrica

- **E’ basata sulle caratteristiche comportamentali del titolare (ritmo, pressione, velocità, accelerazione, movimento, etc.) che firma con uno stilo su una tavoletta grafica.**

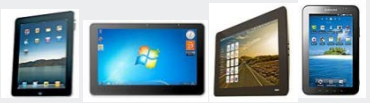
- **Di per sé rappresenta una firma elettronica. Adeguatamente connessa ad un sistema documentale e alle regole previste nel Titolo V delle Regole Tecniche (DPCM 22 febbraio 2013) può divenire una firma elettronica avanzata (FEA).**

- **Se FEA soddisfa il requisito della forma scritta negli scenari di utilizzo più comuni (ma non per il 1350, numeri 1-12 del Codice Civile).**

- **Nei prodotti di mercato viene reso disponibile uno strumento di tipo forense per l’analisi grafologica della sottoscrizione. In tal modo nulla cambia in caso di contestazione della sottoscrizione.**

Caratteristiche dei dispositivi di firma

- I device utilizzati per l'apposizione di firme grafometriche sono **dispositivi hardware dotati di tecnologia touch** in grado di rilevare i principali parametri della firma dell'utente
- E' possibile distinguere **due macro categorie** di dispositivi

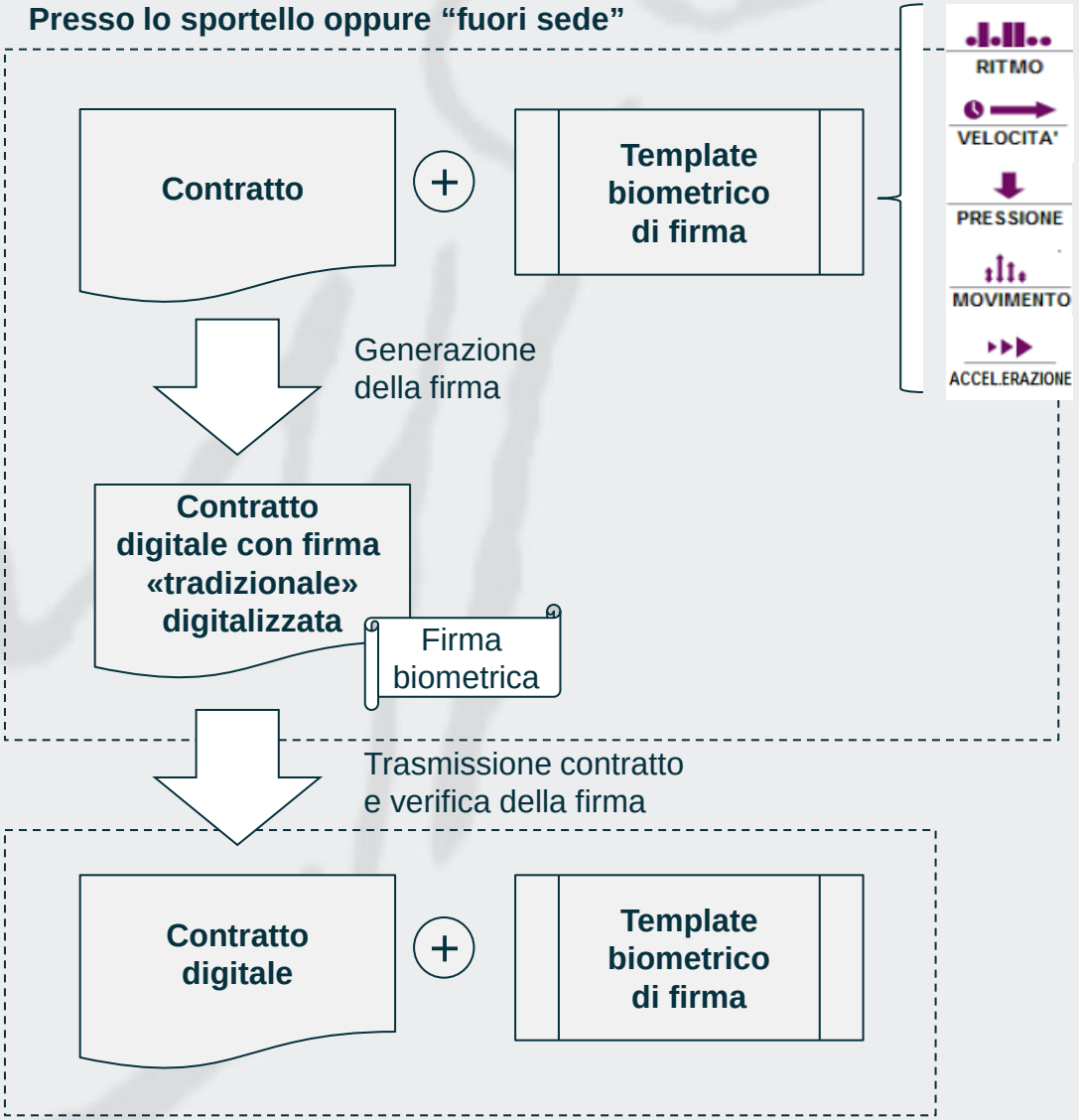
Dispositivi	Caratteristiche	Parametri rilevati
Tablet dedicati	• Dispositivi hardware (tablet) dedicati dotati di tecnologia touch • Postazioni fisse o portatili • Connettività verso pc via USB • Associati a speciali penne per l'apposizione delle firme • Massima accuratezza nella rilevazione dei parametri • Possibilità di impiego per enrollment (prima registrazione parametri di firma) e verifica • Costo tra i 50 e i 600 euro (10") circa in funzione delle caratteristiche del display (b/n vs colori, risoluzione, ecc.)	• Pressione • Velocità • Ritmo • Accelerazione • Movimenti aerei
		
Dispositivi mobili	• Dispositivi mobili dotati di tecnologia touch (es. iPad) • Utilizzo non limitato alla sola apposizione di firme • Connettività verso pc e alla rete • Accuratezza dei parametri rilevati minore rispetto ai device dedicati	• Velocità • Ritmo • Accelerazione • Movimenti aerei
		

L'impossibilità di rilevare la coordinata pressione tramite alcuni dispositivi mobili ne riduce il livello di confidenza

La firma biometrica può essere una firma elettronica avanzata

Caratteristiche

- La firma biometrica è un **processo di calcolo,** legalmente equiparato ad una **firma elettronica avanzata.**
- Si basa sulle caratteristiche grafometriche rilevate **dal tratto a penna** per generare il documento firmato.
- Per elaborare tali caratteristiche (template biometrico), sono usati **specifici devices** – le tavolette di firma - e **software ad-hoc**.
- I parametri biometrici sono allegati al contratto, che **contiene in calce** anche la **firma "tradizionale" a penna** digitalizzata.
- **La validazione** della firma avviene **direttamente in digitale,** confrontando i parametrici biometrici della firma con il profilo della firma "depositato" (in analogia ai cartellini firma "tradizionali")



Firma grafometrica – considerazioni 1/2

- La biometria della firma è basata su ritmo, velocità, pressione, accelerazione e movimento della firma manuale apposta su una tavoletta elettronica (TABLET, PAD).

- In maggiore dettaglio:

  - La velocità di scrittura.
  - La pressione esercitata.
  - L'angolo di inclinazione della penna (se presente la pressione).
  - L'accelerazione del movimento.
  - Il numero di volte che la penna viene sollevata (tratti in aria).

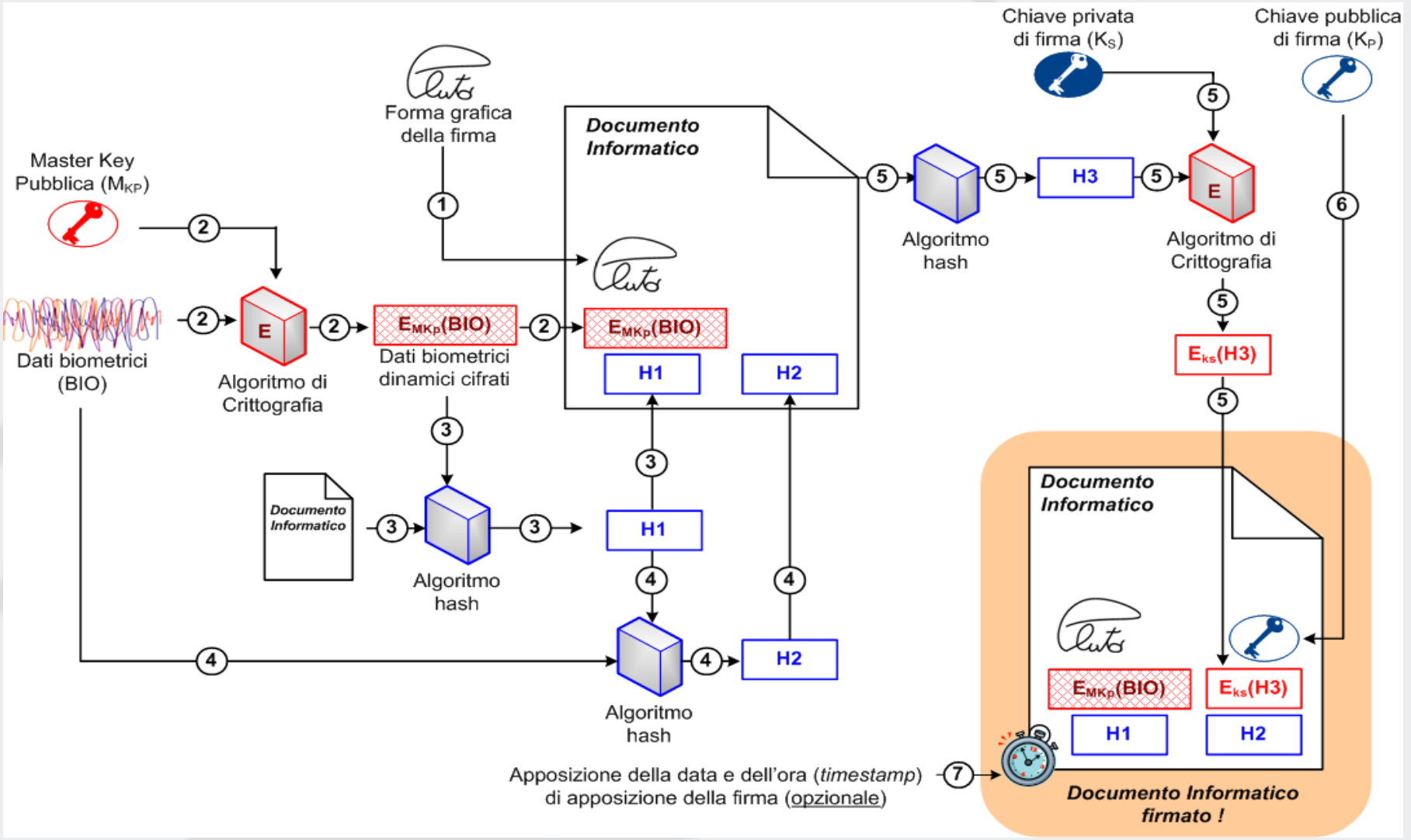
- Quando utilizzata a sportello in presenza di un impiegato o all'interno di un'organizzazione possono essere soddisfatti i requisiti stabiliti per la firma elettronica avanzata.

- Naturalmente è utile essere integrati in un adeguato sistema di gestione documentale.

Firma grafometrica – considerazioni 2/2

- **La firma grafometrica è perfettamente integrabile nelle più diffuse piattaforme di gestione documentale.**
- **E’ possibile effettuare firme multiple sui documenti informatici integrando il workflow documentale con il tool di firma.**
- **Il vantaggio della dematerializzazione “a sportello” è immediatamente percettibile perché il documento nasce digitale, con piena validità legale e con un’accettazione molto elevata da parte dell’utente.**
- **La normativa stabilisce che all’utente vengano illustrati i parametri di sicurezza del sistema.**

Il processo di firma grafometrica



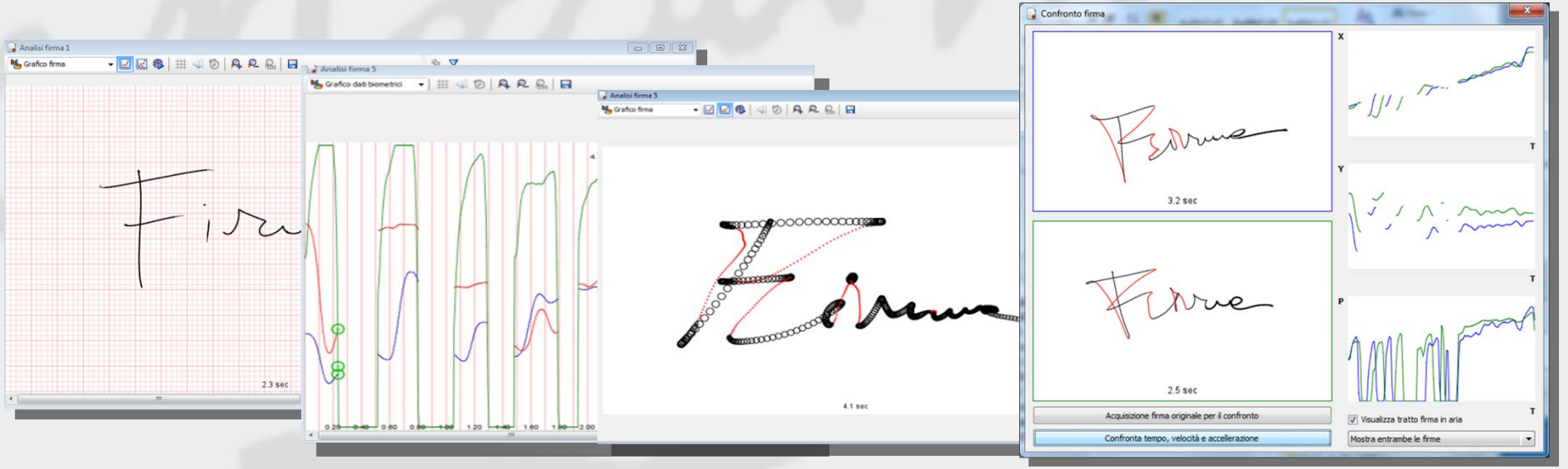
Autore: Mauro Belcastro

Sicurezza del documento sottoscritto

- **H1 (impronta1) serve a garantire un controllo “semplice” sull'integrità e può essere condotto da qualsiasi utente senza disporre di informazioni segrete mediante il semplice ricalcolo dell'hash.**
- **H2 (impronta2) consente un controllo sull’integrità più “complesso”. La funzione di hash in questo caso riceve in input i dati biometrici in chiaro, quindi deve necessariamente essere elaborata in un ambiente adeguatamente protetto e solo su specifiche autorizzazioni delle parti coinvolte. La Master Key privata (MKS) dovrebbe essere conservata in ambiente sicuro (es. Notaio, CA, HSM, ecc.)**
- **La firma del documento viene effettuata con la classica tecnica delle chiavi asimmetriche. Anche in questo caso esistono diverse soluzioni tecnologiche dei Fornitori in merito alla creazione delle chiavi K_P e K_S .**
- **Per la protezione del dato biometrico si consiglia:**
  - Eseguire la cifratura del dato biometrico direttamente all’interno della tavoletta;
  - Cancellare in modo sicuro il dato biometrico non appena eseguita la cifratura.

Firma grafometrica e grafologia forense

- La perizia grafica su base grafologica è una tecnica utilizzata da anni in particolar modo in ambito giudiziario per definire e distinguere la produzione grafica di un individuo da quella di qualsiasi altro.
- In questo contesto la firma grafometrica semplifica di molto l'indagine, in quanto fornisce un maggiore numero d'informazioni rispetto a quelle che si otterrebbero sul cartaceo. Inoltre mentre su supporto cartaceo l'operazione di confronto risente della soggettività dell'osservatore, nella firma grafometrica i dati sono numerici e quindi oggettivi.



DPCM 22 febbraio 2013 – Titolo V

- **Il Titolo V del DPCM recante le regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali è interamente dedicato alla firma elettronica avanzata (FEA).**

- **I soggetti che erogano soluzioni di FEA (soggetti di tipo a) sono coloro che erogano soluzioni di FEA al fine di utilizzarle nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali, realizzandole in proprio o avvalendosi di soluzioni realizzate da soggetti, quale oggetto realizzano soluzioni di FEA a favore degli erogatori di soluzioni. (Art. 55, comma 2 del DPCM).**

- **Gli obblighi a carico dei soggetti che erogano soluzioni di FEA sono contenuti nell'articolo 57 del DPCM.**

I DOVERI DI INFORMAZIONE NEI CONFRONTI DEL FIRMATARIO.

Le informazioni nei confronti del firmatario - 1

- **I soggetti di tipo «a»:**
  - **identificano in modo certo l'utente tramite un valido documento di riconoscimento;**
  - **informano l'utente in merito agli esatti termini e condizioni relative all'uso del servizio che utilizza la FEA. Eventuali limitazioni d'uso sono comprese in questa informativa;**
  - **subordinano l'attivazione del servizio alla sottoscrizione da parte dell'utente di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;**
  - **conservano per almeno venti anni copia del documento di riconoscimento e l'informativa;**

Le informazioni nei confronti del firmatario - 2

- **conservano ogni altra informazione atta a dimostrare l'ottemperanza delle garanzie di conformità alle caratteristiche di FEA. Le informazioni hanno garanzia di disponibilità, integrità, leggibilità e autenticità;**

- **forniscono liberamente e gratuitamente al firmatario, copia della dichiarazione e le informazioni di ottemperanza, su richiesta di questo;**

- **rendono note le modalità con cui effettuare le richieste descritte. Tali modalità sono sul sito internet del soggetto di tipo «a»;**

- **rendono note le caratteristiche del sistema realizzato atte a garantire le conformità alle caratteristiche di FEA;**

Le informazioni nei confronti del firmatario - 3

- **specifica le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto;**
- **le informazioni descritte nei due punti precedenti sono pubblicate sul sito internet del soggetto di tipo «a»;**
- **assicura, ove possibile, la disponibilità di un servizio di revoca del consenso all'utilizzo della soluzione di FEA e di un servizio di assistenza.**

- **Altri obblighi specifici sono descritti nel seguito**

L’OBBLIGO DI PREVENTIVA ACCETTAZIONE DA PARTE DEL FIRMATARIO.

L’obbligo di preventiva accettazione

- **Come abbiamo visto il firmatario accetta la soluzione di FEA in modo esplicito.**

- **Ne consegue che l’adesione deve essere in linguaggio chiaro e non ambiguo. L’utilizzo della firma grafometrica deve essere ben esplicitato rispetto agli scopi legali della sottoscrizione, anche con i limiti d’uso del servizio e le misure di sicurezza adottate per proteggere i dati biometrici della firma nell’ambito del suo completo ciclo di vita.**

- **Non è obbligatorio sottoscrivere l’adesione con la penna visto che l’atto di sottoscrivere non obbliga al cartaceo.**

- **Anche se pochi, alla data si fidano, sarebbe possibile utilizzare la grafometrica per sottoscrivere l’atto.**

I LIMITI D’USO E LE COPERTURE ASSICURATIVE.

I limiti d’uso

- **Come è ovvio i limiti d’uso sono strettamente collegati al servizio di sottoscrizione accettato dall’utente.**
- **Conviene per motivi di trasparenza esplicitare bene i limiti d’uso all’interno della dichiarazione di accettazione.**
- **L’utente potrebbe infatti non disconoscere l’adesione al servizio ma invocare il fatto che quanto gli è stato fatto sottoscrivere nell’accettazione era poco chiaro, incompleto, ambiguo, ecc.**
- **I limiti d’uso quindi devono indicare cosa sto sottoscrivendo e in che spazio queste sottoscrizioni sono circoscritte.**

Gli obblighi di copertura assicurativa

- **Al fine di proteggere i titolari della FEA e i terzi da eventuali danni cagionati da inadeguate soluzioni tecniche i soggetti di tipo «a» si dotano di una copertura assicurativa per la responsabilità civile rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali.**

- **L'ammontare della copeertura è obbligatoriamente non inferiore a 500.000 euro.**

- **Le modalità scelte per la copertura sono pubblicate, ai fini di trasparenza informativa, anche sul proprio sito internet.**

- **Per poco chiari motivi di semplicità l'assicurazione NON è obbligatoria per le persone giuridiche pubbliche che erogano soluzioni di FEA per conto di pubbliche amministrazioni.**

L’adesione nelle PPAA

- **Nell’ambito delle pubbliche amministrazioni e in ambito sanitario limitatamente alla categoria di utenti rappresentata dai cittadini fruitori di prestazioni sanitarie si possono applicare delle semplificazioni in ambito adesione.**

- **Infatti, la dichiarazione di accettazione delle condizioni del servizio può essere fornita oralmente dall’utente al funzionario pubblico o all’esercente la professione sanitaria, il quale la raccoglie in un documento informatico che sottoscrive con firma elettronica qualificata o firma digitale.**

- **Non sono previste semplificazioni per la conservazione ventennale del documento di riconoscimento.**

Altre norme tecniche

- La sicurezza della FEA grafometrica può essere assicurata mediante una certificazione ISO/IEC 27001.
- Tale certificazione è obbligatoria per chi fornisce le PPAA.
- I soggetti di tipo «a» al fine di dare evidenza del grado di conformità della soluzione di FEA a quanto previsto dal DPCM 22 febbraio 2013, su base volontaria, possono far certificare la soluzione in conformità all'ISO/IEC 15408, livello EAL 1.
- La norma ISO è anche nota come Common Criteria.
- Il Garante Privacy ha stabilito altre regole nel Provvedimento 513/2014. Tra le quali quelle che riguardano la gestione della master key. Questa è la componente privata della coppia utilizzata per la protezione dei dati biometrici nel documento.

Gli obblighi di conservazione digitale

- **La produzione di documenti informatici rende obbligatoria la loro conservazione digitale conforme alle specifiche Regole Tecniche (DPCM 3 dicembre 2013).**

- **I tempi di conservazioni sono stabiliti da obblighi di natura fiscale o, per la firma qualificata da esigenze di riferimenti temporali opponibili ai terzi.**

- **Nel caso della firma grafometrica non ci sono particolari obblighi legati ai riferimenti temporali.**

- **Peraltro è molto opportuno conservare i documenti digitali per motivi legati all'integrità, leggibilità e autenticità dei documenti .**

- **Altri motivi potrebbero scaturire dal procedimento utilizzato per la produzione delle FEA grafometrica. Ad esempio esistono soluzioni di mercato che legano la FEA a firme digitali o qualificate.**

LE APPLICAZIONI OPERATIVE NEI DIVERSI SETTORI (BANCARIO, FINANZIARIO, ASSICURATIVO, PPAA, ECC.).

Applicazioni bancarie

- **Dematerializzazione delle procedure in filiale e in mobilità.**
- **Coinvolgimento sia di documenti contabili che contrattuali (forma scritta *ad substantiam*).**
- **Utilizzo sia su postazione fissa che mobile.**
- **Personal computer o tablet.**
- **Diffusione elevata anche di iPAD (dove si perdono alcuni parametri biometrici di base con conseguenze sull'analisi forense).**

Applicazioni finanziarie

- **Dematerializzazione delle procedure in filiale e in mobilità.**
- **Coinvolgimento sia di documenti contabili che contrattuali (forma scritta *ad substantiam*).**
- **Utilizzo su postazione prevalentemente mobile.**
- **Prevalenza di tablet per i *private banker***
- **Minore diffusione di iPAD.**

Applicazioni assicurative

- **Dematerializzazione delle procedure in filiale e in mobilità.**
- **Sottoscrizione delle polizze (forma scritta *ad substantiam*).**
- **Utilizzo sia su postazione fissa che mobile.**
- **Personal computer o tablet.**
- **Diffusione molto elevata anche di iPAD con scelte razionali di non acquisizione della pressione e dei salti in volo del tratto. L'analisi del rischio applicativo rende poco critica la mancanza di questi parametri in fase «forensic».**

Applicazioni nelle PPAA

- **Diffusione limitata.**
- **I CAF la utilizzano ma l'impatto sulle dichiarazioni fiscali è indiretto.**
- **Applicazioni di firma solo grafica in INPS per i medici «fiscali».**
- **Qualcosa in INAIL.**
- **E nelle Università pochissimo.**

Conclusioni

- **Si mantiene alta l'attenzione per le applicazioni grafometriche.**
- **E' in ulteriore crescita l'offerta di software e hardware.**
- **E' ancora limitata l'attenzione sulla grafometria in settori differenti da quelli bancario, finanziario, assicurativo. Ma ci sono timidi segnali in INPS e INAIL e in qualche ente locale.**
- **I vincoli operativi nell'attuazione della FEA stabiliti nelle Regole Tecniche del DPCM 22 febbraio 2013 dovrebbero essere semplificati.**
- **Anche il Provvedimento prescrittivo sulla biometria del Garante Privacy, di grande utilità ed efficacia, dovrebbe essere aggiornato.**

Contatti

Giovanni Manca
e-mail:
mncgnn59@gmail.com