in collaborazione con:

IL DECALOGO DELLA FIRMA GRAFOMETRICA (TRE ANNI DOPO)

I dieci requisiti indispensabili (e aggiornati) per una soluzione efficiente, sicura e rispettosa della privacy

di Giovanni Manca (Comitato Scientifico AIFAG) e Luigi Foglia (Digital & Law Department - Referente territoriale ANORC)

AIFAG Associazione Italiana Firma Elettronica Avanzata Biometrica e Grafometrica
Sede Legale: via Mario Stampacchia 21 - 73100 Lecce - C.F: 93124220752 - E-mail: info@aifag.it

INTRODUZIONE

Il primo decalogo della firma grafometrica, pubblicato nel febbraio del 2012, fu scritto per fissare le idee su questa nuova tecnologia che avanzava in modo dirompente e confuso, per stimolare una discussione sulla sua validità tecnologica e soprattutto sulla sua sicurezza.

In tre anni di acqua sotto i ponti n'è passata parecchia e abbiamo visto tante novità, sia hardware che software, il consolidamento normativo, il Regolamento prescrittivo del Garante per la protezione dei dati personali, tanti progetti che, ancora, si diffondono e si sviluppano e molte migliaia di persone che firmano in modalità grafometrica.

In questo documento viene analizzato lo stato dell'offerta e della domanda, allo scopo di comprendere se la normativa viene correttamente applicata, se il titolare è sempre informato e consapevole dello strumento utilizzato e infine se il triennio trascorso è stato foriero di benefici sulla qualità delle soluzioni e sulla conformità alla normativa.

La struttura del decalogo è inalterata rispetto all'analisi di tre anni fa, proprio per consentire al vecchio e al nuovo lettore un confronto tra la situazione odierna e quella dell'inizio del 2012.

Il nuovo decalogo non vuole, anche stavolta, esaurire e risolvere tutti i dubbi su questa materia, ma semplicemente rappresentare un nuovo punto di analisi su un percorso ampiamente sviluppato e che ha ancora molto da dire in materia di aderenza normativa, organizzazione, tecnologia e sicurezza ICT.

PREMESSA

1. Le firme elettroniche e la FEA grafometrica

Nel nostro ordinamento sono disciplinati diversi tipi di firma elettronica, i quali contribuiscono a determinare il valore giuridico e probatorio dei documenti informatici ai quali sono apposti. I sistemi di firma elettronica, in effetti, si differenziano non solo per le diverse tecnologie utilizzate, ma anche per la loro maggiore o minore capacità di assicurare la presenza di tutti gli elementi idonei a garantire sia l'imputabilità giuridica del documento informatico (cioè, la sua provenienza da parte del soggetto firmatario), sia l'integrità e l'immodificabilità del documento in tal modo firmato (così da poter garantire anche al documento informatico la cd. "forma scritta e sottoscritta"). Non esiste, quindi, la firma "migliore" in assoluto, ma ogni tipologia di firma può essere utilizzata in modo appropriato in base al livello di "affidabilità giuridica" che si intende conferire al documento informatico che si sta sottoscrivendo. In effetti, anche la cd. firma elettronica "semplice" può essere astrattamente idonea a far acquistare al documento informatico su cui è apposta il valore di forma scritta in base alle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità del processo attraverso il quale si è formata: la legge richiede al giudice, di volta in volta, di esprimere un giudizio sull'idoneità a soddisfare il requisito della forma scritta e sul relativo valore probatorio di un documento sottoscritto con una firma elettronica semplice, ai sensi dell'art. 20, comma 1 bis, del CAD. Alle altre tipologie di firma elettronica (avanzata, qualificata e digitale), invece, viene riconosciuta la medesima validità della "forma scritta e sottoscritta".

Per quanto riguarda la FEA (firma elettronica avanzata), le Regole tecniche dettate dagli artt. 55 e ss. del DPCM 22 febbraio 2013 stabiliscono che la realizzazione di tali soluzioni di firma elettronica è libera e non è soggetta ad alcuna autorizzazione preventiva. Tanta libertà di scelta in relazione alle tecnologie e i metodi da utilizzare per realizzare una soluzione di FEA è, però, stata mitigata

dalle stesse Regole tecniche già richiamate, in quanto il valore della FEA è limitato al solo contesto in cui essa viene utilizzata (tra il sottoscrittore e il soggetto proponente tale modalità di sottoscrizione), rendendo, tra l'altro, necessario che le sue condizioni di utilizzo siano preventivamente accettate per iscritto dagli utenti/sottoscrittori. Per questi motivi, il soggetto che realizza la soluzione di firma elettronica avanzata, prima di poterla utilizzare per regolare i rapporti intercorrenti con il proprio utente, dovrà correttamente informarlo in merito agli esatti termini e condizioni relativi al servizio, compresa ogni eventuale limitazione dell'uso. In ogni caso, occorre tenere presente che tutto il processo relativo alla firma elettronica avanzata deve essere orientato alla sicurezza delle informazioni trattate; ulteriormente, devono essere garantite l'integrità e la leggibilità dei dati e deve inoltre essere impedito ogni possibile accesso abusivo ai dati stessi (soprattutto quando i dati trattati siano di tipo biometrico).

Sulla scorta di quanto previsto dall'art. 56 delle citate Regole tecniche, di cui al DPCM 22 febbraio 2013, anche i dati biometrici possono essere utilizzati per la generazione delle firme elettroniche avanzate (art. 56, comma 1, lett. c), in particolare perché si tratta normalmente di dati sotto il controllo esclusivo del firmatario. Se accanto a questo si pensa anche al fatto che non è necessario dotare il sottoscrittore di alcun ulteriore dispositivo per poter procedere alla sottoscrizione (smart card, chiavette usb, token otp, etc.), risulta immediatamente percepibile il positivo impatto di questi sistemi in termini di semplificazione per l'utente/sottoscrittore.

Tra le varie firme che è possibile ottenere utilizzando dati biometrici, particolare attenzione meritano le firme grafometriche. Tali firme, infatti, realizzate mediante la memorizzazione dei dati comportamentali dell'utente legati all'apposizione materiale della firma autografa, hanno l'indubbio vantaggio di rendere possibile un'implementazione elettronica della sottoscrizione di un documento, permettendo allo stesso utente di continuare a firmare con modalità molto simili a quelle solitamente usate sulla carta.

2. Il Provvedimento Generale Del Garante

Nel seguito di questo scritto illustriamo in modo sintetico le funzionalità della firma grafometrica secondo l'attuale stato dell'arte. L'analisi tecnica e organizzativa è sviluppata anche alla luce del provvedimento prescrittivo in tema di biometria (n. 513/2014) del Garante per la protezione dei dati personali.

Il provvedimento, riporta un quadro unitario di misure e accorgimenti di carattere tecnico, organizzativo e procedurale necessari per mantenere alti i livelli di sicurezza nell'utilizzo di particolari tipi di dati biometrici, semplificando tuttavia alcuni adempimenti. Tale provvedimento si è reso necessario in seguito all'aumento esponenziale dell'uso di dispositivi e tecnologie per la raccolta e il trattamento dei dati biometrici con la finalità di accertare l'identità personale di un interessato o utente nei casi in cui egli fruisca dei servizi forniti dalla società dell'informazione. Poiché una simile attività potrebbe essere lesiva dei diritti fondamentali dell'interessato, la volontà perseguita dall'Autorità Garante è stata quella di precisare, anche tramite la previsione di un documento "Linee guida in materia di riconoscimento biometrico e firma grafometrica" (allegato al Provvedimento Generale citato), quali siano le operazioni che i titolari del trattamento devono compiere per agire in conformità ai principi previsti dal Codice in materia di protezione dei dati personali e agli standard di sicurezza. Il Garante ha, in tal modo, inteso individuare delle specifiche tipologie di trattamento per le quali, a condizione di applicare tutte le misure necessarie prescritte,

si possa procedere al trattamento senza ulteriormente richiedere alcuna verifica preliminare (come sarebbe normalmente previsto dall'art. 17 del Codice Privacy).

ARCHITETTURA DEI SISTEMI GRAFOMETRICI

Negli ultimi tre anni sono stati sviluppati numerosi sistemi software che consentono una firma grafometrica. Una dozzina (nell'enumerazione non si tiene conto delle specializzazioni del software per i differenti ambienti operativi, ma solo dell'azienda sviluppatrice) di questi sistemi sono stati sviluppati da aziende italiane. In parallelo si è anche ampliato in maniera significativa il mercato dell'hardware in termini di PAD dedicati all'acquisizione grafica e tablet o portatili di uso generale predisposti per l'acquisizione grafica.
In molti casi si può disporre di hardware a utilizzo misto con tastiera rimovibile.
Pur nelle specifiche caratteristiche dei singoli sistemi, l'architettura generale di ciascuno di essi è pressoché la stessa.
Sulla postazione di lavoro fissa o portatile viene installato un software che colloquia con la tavoletta grafica. La connessione tra tavoletta e computer avviene tramite un cavo con interfaccia USB. Se si opera con dispositivo dotato di schermo sensibile ovviamente non c'è bisogno di utilizzare tale tavoletta grafica.
La novità degli ultimi mesi è nella "certificazione" informale, da parte di un paio di aziende, dell'hardware utilizzato per l'acquisizione dei dati di sottoscrizione.
Il dato importante è che perché i sistemi siano approvati non basta che funzionino, ma occorre che superino una serie di test che hanno lo scopo di verificare la qualità dei dati biometrici acquisiti e la loro conseguente fruibilità nell'analisi forense della sottoscrizione (in altre parole la perizia grafologica).
Per parlare di sottoscrizione è necessario disporre di un documento informatico. La quasi totalità degli strumenti di firma utilizza il formato PDF (PDF/A) con la disponibilità di uno o più campi firma, peraltro in qualche contesto la firma grafometrica è stata sperimentata anche su documenti in formato XML.
Il campo firma viene presentato al sottoscrittore in modalità esplicita sul dispositivo.
Nel tempo il mercato ha richiesto sempre di più un'alta "user experience" nella presentazione del documento al sottoscrittore e questo ha sollecitato lo sviluppo e l'offerta di un elevato numero di soluzioni hardware con visualizzazione ad alta risoluzione e di dimensioni pari a 10" circa.
La forte diffusione dell'iPAD, che, come è noto, dispone di sensori a tecnologia capacitiva, ha anche stimolato l'offerta di stilo elettronici in grado di rilevare la pressione:
l'utente sottoscrive il documento e grazie al cosiddetto "ink effect", l'effetto grafico sulla tavoletta e nel campo firma del documento è quello di una classica firma sulla carta.
In termini visivi potremmo anche pensare che la firma catturata sia una semplice scansione dell'originale, ma ovviamente non è così.
La disponibilità del dato pressorio, oltre che aumentare l'effetto positivo sulla "user experience", consente di disporre di un ulteriore dato utile per le eventuali analisi peritali di verifica della sottoscrizione.
Completata la firma, l'utente può decidere di accettarla premendo con la penna un'opzione di conferma o di rifarla annullando l'operazione appena compiuta.

AIFAG Associazione Italiana Firma Elettronica Avanzata Biometrica e Grafometrica
Sede Legale: via Mario Stampacchia 21 - 73100 Lecce - C.F: 93124220752 - E-mail: info@aifag.it

Se l'utente accetta, il documento è compiutamente firmato e si presenta sullo schermo con la sottoscrizione in bella vista nell'apposito campo. Se i sottoscrittori sono più di uno, l'operazione si ripeterà per un numero di volte pari a quello dei sottoscrittori.
Il tempo passato dal debutto di questi sistemi non ha eliminato le perplessità e i dubbi degli scettici, ma anche i numerosi sottoscrittori più ottimisti chiedono:

- garanzie del fatto che la firma non possa essere estrapolata dal contesto e poi utilizzata per firmare altri documenti;
- dettagli sul trattamento del dato biometrico;
- informazioni sulla verificabilità della sottoscrizione in caso di contenzioso.

A tal proposito, un grosso aiuto è stato fornito dal sopra citato provvedimento prescrittivo in tema di biometria del Garante per la protezione dei dati personali.
In questo provvedimento vengono, infatti, stabilite regole molto precise sulla sicurezza del trattamento del dato biometrico e per i trattamenti necessari alla realizzazione di una firma grafometrica.
Realizzare una soluzione aderente al citato provvedimento permette di ritenere sicuro il trattamento realizzato ed evitare, in tal modo, il ricorso a una verifica preliminare da parte del Garante, altrimenti obbligatoria.
Vediamo quindi come le architetture devono operare per rendere sicure le operazioni che abbiamo appena descritto.
Queste regole di conformità sono anche l'attestato di conformità alle regole privacy.

LA SICUREZZA DELLA FIRMA GRAFOMETRICA

In questa fase storica è più opportuno analizzare i requisiti prescritti dal Garante per la protezione dei dati personali piuttosto che ipotizzare un funzionamento dei prodotti di mercato conforme alle regole generali di sicurezza.
Il provvedimento prescrittivo n. 513/2014 affronta in dettaglio il tema della firma grafometrica nel paragrafo 4.4 dedicato alla sottoscrizione dei documenti informatici.
Il Garante giustifica l'utilizzo di tali sistemi sia perché li ritiene in grado di contrastare eventuali tentativi di frode e il fenomeno dei furti di identità e sia perché il ricorso a tali soluzioni permette di rafforzare le garanzie di autenticità e integrità dei documenti informatici sottoscritti, anche in vista di un eventuale contenzioso legato al disconoscimento della sottoscrizione apposta su atti e documenti di tipo negoziale in sede giudiziaria.
Il Garante, inoltre, considera valido il presupposto di legittimità del trattamento biometrico se è stato dato il consenso - effettivamente libero - degli interessati. In ambito pubblico devono essere perseguite le finalità istituzionali del titolare stesso. Il consenso è espresso dall'interessato all'atto di adesione al servizio di firma grafometrica ed è valido, fino alla sua eventuale revoca, per tutti i documenti da sottoscrivere.
L'esonero dall'obbligo di presentazione dell'istanza di verifica preliminare (art. 17 della 196/2003) da parte del titolare del trattamento è applicabile se questo è svolto nel rispetto delle prescrizioni e limitazioni riportate di seguito estratte direttamente dal Provvedimento del Garante:

a) il firmatario può sottoscrivere solo a fronte di identificazione. Questa prescrizione è identica a quella dell'art. 57, comma 1, lettera a) del DPCM 22 febbraio 2013.

b) Sono resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici.

c) La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo il completamento della procedura di sottoscrizione, e nessun dato biometrico persiste all'esterno del documento informatico sottoscritto.

d) I dati biometrici e grafometrici non sono conservati, neanche per periodi limitati, sui dispositivi hardware utilizzati per la raccolta, venendo memorizzati all'interno dei documenti informatici sottoscritti in forma cifrata tramite sistemi di crittografia a chiave pubblica con dimensione della chiave adeguata alla dimensione e al ciclo di vita dei dati e certificato digitale emesso da un certificatore accreditato ai sensi dell'art. 29 del Codice dell'amministrazione digitale. La corrispondente chiave privata è nella esclusiva disponibilità di un soggetto terzo fiduciario che fornisca idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave. La chiave può essere frazionata tra più soggetti ai fini di sicurezza e integrità del dato. In nessun caso il soggetto che eroga il servizio di firma grafometrica può conservare in modo completo tale chiave privata. Le modalità di generazione, consegna e conservazione delle chiavi sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1 lettere e) ed f) del DPCM 22 febbraio 2013.

e) La trasmissione dei dati biometrici tra sistemi hardware di acquisizione, postazioni informatiche e server avviene esclusivamente tramite canali di comunicazione resi sicuri con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati.

f) Sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione delle postazioni informatiche e dei dispositivi, se non esplicitamente autorizzati.

g) I sistemi informatici sono protetti contro l'azione di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati.

h) Nel caso di utilizzo di sistemi di firma grafometrica nello scenario mobile o BYOD (Bring Your Own Device), sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili, con il ricorso a strumenti MDM (Mobile Device Management) o MAM (Mobile Application Management) o altri equivalenti al fine di isolare l'area di memoria dedicata all'applicazione biometrica, ridurre i rischi di installazione abusiva di software anche nel caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (malware).

i) I sistemi di gestione impiegati nei trattamenti grafometrici adottano certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro (in particolare, rendendo disponibili funzionalità di remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi).

j) L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, o da più soggetti, in caso di frazionamento della chiave stessa, e nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma e a seguito di richiesta dell'autorità giudiziaria. Le condizioni e le

modalità di accesso alla firma grafometrica da parte del soggetto terzo di fiducia o da parte di tecnici qualificati sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1, lettere e) ed f) del DPCM 22 febbraio 2013.

k) E' predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità. Tale relazione tecnica è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante.

I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica ISO/IEC 27001:2005 e successive modificazioni che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico."

A questo punto sono utili alcuni commenti sui singoli punti sopra riportati.
L'obbligo di adesione al servizio di firma grafometrica, insieme alla prescrizione del Garante di un metodo alternativo (digitale o cartaceo) senza dati biometrici, crea un problema a quelle organizzazioni che vogliono eliminare totalmente il supporto cartaceo.
Questo porta a pressioni più o meno esplicite sul sottoscrittore per aderire al servizio senza aver accettato con un adeguato livello di consapevolezza quanto previsto dalle norme.
Seppur raramente, capita anche che non vi siano nemmeno richieste di adesione o di consensi al trattamento del dato biometrico; nessun problema, invece, per le acquisizioni informatiche del solo tratto grafico della sottoscrizione che non è considerato un dato biometrico.
Per quanto attiene alla cancellazione dei dati biometrici questa è sempre legata alla dichiarazione del fornitore della soluzione. In assenza di valutazioni di sicurezza condotte da terzi nell'ambito di test conformi ai Common Criteria, non si hanno alternative alle dichiarazioni dei produttori.
Le altre prescrizioni sono tipiche per la sicurezza ICT anche in ambiente mobile o di tipo BYOD. In questi ultimi casi la disponibilità di software MDM o MAM appare utile in senso generale e non specificatamente per il contesto biometrico, in quanto questo tipo di dato viene immediatamente protetto con le chiavi crittografiche del sistema (master key).
Nella gestione della master key sono chiare le prescrizioni operative ma, presumibilmente, in risposta a istanze di verifica preliminare sarà chiarita la figura di soggetto terzo fiduciario: in particolare se questa figura possa coincidere con il certificatore accreditato che genera il certificato o se, nella stretta interpretazione della figura di terzo, egli debba essere un soggetto diverso dal certificatore sopra citato.

L'INTEGRITÀ DEL DOCUMENTO SOTTOSCRITTO

Rispetto al passato, l'integrità del documento sottoscritto viene garantita con l'opportuno utilizzo di funzioni di hash e il relativo calcolo di impronte. In tal modo viene data la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma, così come previsto dalla lett d) del comma 1 dell'art. 56 del DPCM 22 febbraio 2013.
Si ricorda che l'impronta è diversa per ogni documento e non è possibile, allo stato attuale delle conoscenze, produrre un documento diverso dall'originale con la stessa impronta.

I dettagli di queste tecnologie sono sempre gelosamente custoditi dalle aziende produttrici dei sistemi grafometrici e rispetto all'articolo di tre anni fa non è possibile aggiungere nulla di maggiormente certo o dettagliato.
Il fatto che l'integrità del documento sottoscritto è garantita con metodi proprietari impedisce, di fatto, la standardizzazione di metodi di verifica della firma grafometrica.
Peraltro, la prescrizione del Garante per la protezione dei dati personali, che prevede la disponibilità dei dati biometrici solo a seguito di richieste dell'autorità giudiziaria, rende il tema non critico nella pratica operativa.
Spesso l'utilizzo di una firma digitale apposta mediante un certificato qualificato del proponente la soluzione di FEA o l'immediato versamento in un sistema di conservazione contribuiscono ulteriormente a garantire una rapida e semplice verifica dell'integrità del documento sottoscritto.

LA VERIFICA DELLA FIRMA GRAFOMETRICA

La verifica della firma grafometrica può avvenire solo se effettuata direttamente sul dato biometrico decifrato e solo su richiesta/autorizzazione dell'autorità giudiziaria. In tal senso, il ruolo del terzo depositario della master key diventa di fondamentale importanza al fine di garantire la corretta disponibilità dei dati biometrici al perito autorizzato alla loro verifica.
Contemporaneamente allo sviluppo di sistemi di firma grafometrica, si sono affermati strumenti analitici (tool grafotecnici) a supporto del perito in tribunale.
Proprio perché è il perito a dover fare l'analisi finale è sostanzialmente decisiva, per attribuire la corretta titolarità della sottoscrizione grafometrica, la qualità dello strumento di analisi forense.
Sul mercato sono disponibili prodotti giudicati ufficialmente adeguati da associazioni professionali o da singoli periti di adeguata fama ed esperienza.
Non solo l'adeguatezza di tali strumenti ma anche la loro disponibilità (almeno fino all'approvazione di uno standard dedicato alla rappresentazione del dato grafometrico) diventa quindi di fondamentale importanza.

IL DECALOGO DEI REQUISITI

Il decalogo dei requisiti viene presentato con una cronologia logica che parte dall'hardware di acquisizione (la tavoletta grafica) e si chiude con la visione aggiornata dello scenario commerciale.
Il decalogo ancora una volta non esaurisce tutti gli aspetti sotto analisi, ovvero non è la base per una valutazione esaustiva delle soluzioni disponibili, ma consente comunque di focalizzare gli aspetti cruciali della soluzione che si analizza, al fine dell'utilizzo della stessa in piena conformità con le norme tecniche e le prescrizioni in materia di privacy.

1) LE CARATTERISTICHE DEL TABLET

Non utilizzare hardware non specificamente testato dal proprio fornitore di software grafometrico. Le sorprese in caso di contenzioso e di conseguente analisi forense del perito grafologo potrebbero essere poco piacevoli.

2) LA SICUREZZA DEL COLLOQUIO TABLET-PC

Il tema si applica nel caso di PAD incorporato nel dispositivo mobile o nel notebook.

Prima bisognava prestarci attenzione perché era corretto in termini di sicurezza informatica, adesso perché altrimenti si viola la normativa sulla protezione dei dati personali e, come è noto, le sanzioni possono essere pesanti.

Il soggetto che eroga la soluzione di firma elettronica avanzata basata su tecniche grafometriche (art. 55, comma 2, lettera a) del DPCM 22 febbraio 2013) dovrebbe sempre disporre di una nota tecnica, prodotta dal fornitore della soluzione, che assicuri la conformità di quest'ultima alla normativa vigente.

3) LA FIRMA ALL'INTERNO DEL DOCUMENTO INFORMATICO

L'evoluzione dei prodotti ha sviluppato numerose soluzioni tecniche nuove, con scopi analoghi a quelli descritti in precedenza ma sempre poco note al soggetto erogatore. Nei prossimi mesi sarà disponibile una proposta tecnica che consente di disporre dei dati biometrici in formato conforme alla specifica ISO/IEC 19794-7: ciò consentirà di analizzare il dato biometrico (dopo la richiesta dell'autorità giudiziaria) da un qualunque strumento di analisi grafometrica che aderirà alle specifiche di formato.

4) LA GESTIONE E PROTEZIONE DELLA MASTER KEY

Nel provvedimento prescrittivo 513/2014 il Garante per la protezione dei dati personali fornisce una serie di regole da seguire con diligenza. Nel breve periodo qualche risposta da parte del Garante a istanze di verifica preliminare potrebbe chiarire meglio il ruolo e la figura del soggetto terzo fiduciario.

5) LA GESTIONE DEI DATI TEMPORANEI

Su questo tema bisogna fidarsi del fornitore, questo almeno fino a quando non sarà utile per il mercato avere a disposizione un profilo di sicurezza condiviso anche istituzionalmente che induca gli operatori di mercato a investire nella certificazione Common Criteria. Purtroppo oggi il profilo richiesto dal potenziale cliente non attribuisce alcun particolare valore a questa caratteristica e quindi il mercato non investe perché ritiene (giustamente) che siano soldi sprecati.

E l'investimento è di alcune decine di migliaia di euro.

6) GLI STRUMENTI PER L'ANALISI GRAFOLOGICA

La disponibilità di uno strumento per l'analisi grafologica è ormai standard nella fornitura di soluzioni di FEA basate su tecnologie grafometriche. Un paio di prodotti hanno raggiunto un elevato livello di qualità per quanto attiene alle modalità offerte al perito per l'analisi.
Alcuni prodotti sono stati valutati direttamente da periti specializzati e consulenti dei tribunali. Un prodotto è stato valutato positivamente e giudicato conforme alle modalità operative professionali da una primaria associazione nazionale di grafologi.
Al fine di ovviare a successivi problemi di sicurezza delle chiavi utilizzate, si inizia a ragionare sull'utilità di inserire alcune funzioni nei software di verifica in grado di permettere la gestione di chiavi asimmetriche di cifratura da utilizzare per la comunicazione sicura del dato grafometrico. In tal modo si potrebbe aiutare a garantire la gestione in sicurezza dei dati grafometrici da parte del perito senza inficiare la sicurezza della master key custodita dalla terza parte fidata (che in tal modo non verrebbe mai rivelata) e assicurandone comunque una comunicazione sicura. In pratica lo scambio dei dati grafometrici avverrebbe mediante loro decifrazione e nuova cifratura (stavolta con la chiave pubblica fornita dal perito) da parte del terzo custode ed essi sarebbero trasmessi al perito che li elaborerebbe in chiaro mediante l'utilizzo della sua chiave privata.

7) LA VERIFICA DELLA FIRMA: FAR E FRR

Visti gli sviluppi della firma grafometrica come equivalente alla firma autografa - e quindi la non necessità di verifica dinamica della sottoscrizione - il tema delle soglie di falsa accettazione (FAR) e di falso rigetto (FRR) non è importante. Questo perché nella maggior parte dei casi ci si è mossi verso la verifica statica della sottoscrizione e quindi verso l'utilizzo del grafologo. Rimane comunque importante la verifica dinamica commentata al punto seguente.

8) LA VERIFICA DELLA FIRMA: SERVER ANONIMO

In alcuni progetti la firma grafometrica viene utilizzata come strumento di identificazione informatica del titolare. In questo caso la firma è stata depositata su un server e viene gestita in modalità anonima. Il sottoscrittore è già identificato e quindi la firma, se correttamente verificata, ha generalmente lo scopo di abilitare una firma qualificata remota.
Con il provvedimento prescrittivo del Garante per la protezione dei dati personali i progetti basati su questa architettura tecnologica devono obbligatoriamente essere approvati a seguito di un'istanza di verifica preliminare ai sensi dell'articolo 17 del Codice privacy (D.LGS. 196/2003).

9) LA CONFORMITÀ ALLE REGOLE TECNICHE NAZIONALI

In questa sede ci si riferisce prevalentemente a quanto prescritto dall'art. 57 del DPCM 22 febbraio 2013. Gli obblighi stabiliti in questa sede sono spesso assolti in modo superficiale e quindi insufficiente rispetto agli scopi che si è prefisso il legislatore. Spesso l'adesione al servizio viene sottoscritta dal titolare sotto la pressione del soggetto erogante ovvero non viene fornita adeguata informazione sul servizio stesso.
In modo analogo quanto prescritto dall'articolo 57, comma 1, lettere e) ed f) viene pubblicato sul sito internet del soggetto erogante la soluzione di FEA in modo generico e spesso con un profilo descrittivo di taglio commerciale, piuttosto che riferito ai principi di conformità della soluzione e a quanto stabilito nel sopra citato DPCM.
Una non corretta comunicazione e informazione in relazione alla soluzione adottata rappresenta, però, un rischio per lo stesso soggetto proponente la soluzione di FEA nel momento in cui l'azione giudiziaria dovesse puntare non tanto al classico disconoscimento della firma grafometrica ma, piuttosto, alla dimostrazione della non conformità della soluzione proposta alle regole tecniche per le FEA: il rischio, in tal caso, sarebbe quello di un degradamento della firma (da avanzata a semplice) con la conseguenza di un non pieno riconoscimento del suo valore giuridico e probatorio e la possibilità che vengano considerati nulli gli atti sottoscritti nei casi in cui sia richiesta la forma scritta e questo requisito non sia stato ritenuto comunque soddisfatto dal giudice .

10) LA CULTURA DEI FORNITORI

La forte richiesta da parte del mercato ha affollato lo stesso di un numero elevato di soluzioni hardware e software. La semplice presentazione di un documento di test e l'immediata comparsa della propria firma sul display rende affascinante questo tipo di soluzioni.
I fornitori continuano a essere o artigiani del prodotto o rivenditori di soluzioni di altri. Nel primo caso spesso ci si trova di fronte a bravi programmatori con scarsissima cultura normativa, mentre nel secondo abbiamo rivenditori in senso stretto con scarsa conoscenza della tecnologia offerta.

AIFAG Associazione Italiana Firma Elettronica Avanzata Biometrica e Grafometrica
Sede Legale: via Mario Stampacchia 21 - 73100 Lecce - C.F: 93124220752 - E-mail: info@aifag.it

In ogni caso nel triennio trascorso l'affidabilità e la qualità dei fornitori è significativamente aumentata, anche se ancora non a un livello tale da essere giudicata complessivamente come ottima.

CONCLUSIONI

Nel presente articolo è stato presentato un quadro sintetico dell'architettura funzionale della firma grafometrica.
Sono stati evidenziati i principali meccanismi di sicurezza sia nell'apposizione che nella verifica della FEA, anche alla luce delle recenti prescrizioni del Garante per la protezione dei dati personali.
Tutti i punti del decalogo (che, lo ribadiamo, sono gli stessi della versione del 2012) sono ancora di attualità, salvo quello sul FAR e FRR (punto 7) che sono attualmente di scarso interesse.
Il provvedimento del Garante per la protezione dei dati personali n. 513/2014 ha confermato molte indicazioni sulla sicurezza e protezione del dato biometrico; le regole indicate in tale provvedimento dovranno essere applicate ma soprattutto sarà importante l'attività ispettiva sulla loro reale applicazione.
La firma grafometrica si conferma molto più sicura di quanto pensano gli scettici ma ancora presenta delle funzionalità poco chiare, sia perché esso non sono adeguatamente e esaustivamente descritte dai fornitori, sia perché mancano analisi e pubblicazioni condotte da terze parti sulla reale conformità delle soluzioni.
Nella diffusione della firma grafometrica è ancora poco applicato un adeguato approccio organizzativo sulle modalità di utilizzo e sui processi di sicurezza che devono essere messi in campo per le operazioni di attivazione delle postazioni di lavoro o durante la verifica delle firme con i dati biometrici decifrati.
Purtroppo molto spesso le regole organizzative a norma di legge sono carenti e l'adesione del titolare è poco consapevole e seguente a pressioni dell'organizzazione erogante.
La certificazione Common Criteria della soluzione di firma grafometrica è sempre valutata dalle principali aziende di settore ma la richiesta blanda (per non dire nulla) del mercato, il costo di valutazione ampiamente a quattro zeri, ma anche la mancanza di un chiaro e condiviso perimetro di certificazione non l'hanno resa una prassi nell'evoluzione dei prodotti di grafometria.
Ancora una volta è utile sottolineare che la storia dei prodotti innovativi con forti implicazioni di sicurezza ICT insegna che sottovalutare la sicurezza non lascia alternative a spiacevoli perdite di dati e anche a conseguenti sanzioni.
Se ci sono falle di sicurezza, queste prima o poi vengono a galla e spesso in modo irrimediabile.
Le dichiarazioni di sicurezza del fornitore non possono bastare per una reale e ragionevole garanzia di sicurezza ai fini della qualità del servizio e soprattutto della conformità alla normativa vigente.

AIFAG Associazione Italiana Firma Elettronica Avanzata Biometrica e Grafometrica
Sede Legale: via Mario Stampacchia 21 - 73100 Lecce - C.F: 93124220752 - E-mail: info@aifag.it