A.G.I.
ASSOCIAZIONE GRAFOLOGICA ITALIANA

POLIZIA SCIENTIFICA

Namirial

Linee guida operative per la verifica della firma biometrica con tecnologia grafometrica in ambito peritale

v.2.2

1. Elenco Versioni

Versione	Data	Descrizione Modifica
1.0	15/12/2021	Prima stesura
2.0	12/02/2022	Seconda revisione. Impaginazione grafica,
2.1	18/02/2022	Terza revisione. Modifica contenuti
2.2	15/06/2022	Quarta revisione. Modifica contenuti

2. LINEE GUIDA – FIRMA BIOMETRICA-GRAFOMETRICA

Documento redatto in collaborazione con:

- A.G.I. (Associazione Grafologica Italiana) – Dipartimento Peritale[1];
- Namirial SpA[2];
- Servizio Polizia Scientifica di Roma[3].

3. PREMESSA

La grafometrica è una tecnologia che può essere utilizzata per acquisire firme o testi. Nello specifico la firma grafometrica prevede l'operazione di sottoscrizione, utilizzando una penna attraverso un apposito device. Questi dispositivi, utilizzando una stilo attiva (alimentata) o passiva (non alimentata), sono in grado di rilevare i dati biometrici della firma:

- Pressione del tratto;
- Posizione in termini di coordinate X,Y (assi orizzontali e verticali);
- Tempo impiegato

Oltre a:

- Rappresentazione grafica.

I dati vengono rilevati con una frequenza di campionamento definita dal produttore. Questi dati, opportunamente cifrati attraverso la chiave pubblica di un certificato di cifratura, vengono poi inseriti all'interno di un file pdf utilizzando le potenzialità della firma PadEs.

Oltre ai dati biometrici suddetti è possibile rilevare:

- Tratti a pressione zero;
- Tratti in volo qualora il dispositivo di firma sia di tipo EMR;

nonché calcolare:

[1]Coordinatore Dipartimento Peritale A.G.I. – Dott.sa Patrizia Pavan
Dipartimento Peritale A.G.I. – Daniela Mazzolini
[2] Vertical Software Product Director – Esperto tecnologia firma grafometrica – Ing. Luigi Enrico Tomasini
[3] Direttore del Servizio Polizia Scientifica – Dirigente Superiore della Polizia di Stato – Dr. Luigi Rinella
Direttore della III Divisione – Primo Dirigente Tecnico della Polizia di Stato – Dr.ssa Antonietta Lombardozzi
Direttore Tecnico Superiore della Polizia di Stato – Dr. Gianluca Tarei
Commissario della Polizia di Stato – Dr. Simone Longo
Ispettore della Polizia di Stato – Maria Vincenza Caria
Ispettore della Polizia di Stato – Aloisi Maria Concetta
Ispettore della Polizia di Stato – Daniela Pappacena
Ispettore della Polizia di Stato – Marco Pagano
Assistente Capo Coordinatore della Polizia di Stato – Adele Santoro
Assistente Capo Coordinatore della Polizia di Stato – Ugo Arcuri

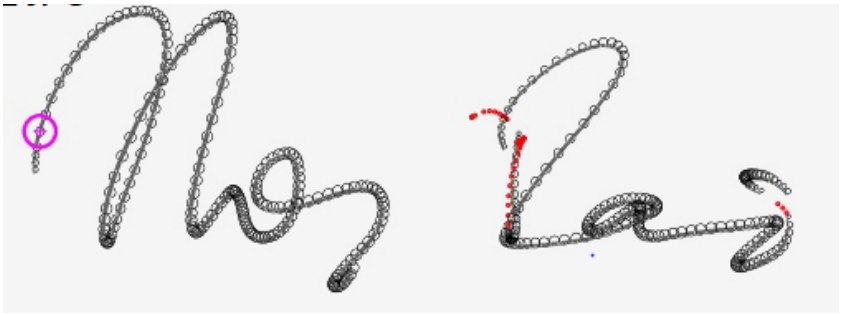
- Velocità
- Accelerazione.

Il principale motivo della diffusione di questa tecnologia è legato al fatto che la firma grafometrica richiama l'operatività di una firma autografa, con apposizione manuale del tratto, senza repentini impatti tecnologici sugli utenti firmatari. A differenza della firma autografa, vengono conservati anche tutti i dati oggettivi suddetti, che permettono di ricondurre al firmatario la sottoscrizione.

Nel processo di raccolta dei dati gioca un ruolo fondamentale la figura di una Terza Parte fidata, incaricata di conservare parte, o tutto il controllo della chiave privata usata per decifrare i dati biometrici del firmatario, che possono essere accessibili solo nei casi di procedure giudiziarie.
La soluzione di firma grafometrica deve rispettare i vincoli imposti dalle norme sulla protezione dei dati personali (regolamento europeo GDPR e coordinamento nazionale con la il decreto 101/2018), seguendo le regole del Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014 del Garante privacy nazionale.
La firma grafometrica applicata in diversi contesti, può essere classificata come Firma Elettronica Semplice o Firma Elettronica Avanzata. La differenza sta nel processo al cui interno è inserita l'operatività, da parte di chi decide di adottare la soluzione.

Il tratto grafico apposto come immagine nel file pdf è in realtà una rappresentazione della firma stessa. Ogni *tot* millisecondi, a seconda della frequenza di campionamento, vengono rilevati i dati biometrici. I singoli tratti collegati tra di loro generano una rappresentazione verosimilmente fedele della firma, che può essere utilizzata al pari di una fotocopia di un documento contenente una firma autografa.

E' utile sapere se siano stati applicati algoritmi di interpolazione o di smoothing grafico.



4. VERIFICHE

4.1 Stragiudiziale – Documento "PDF flat" (definizione BPM ENFSI, versione 03, ottobre 2020

I risultati e l'attendibilità dell'esame di un documento, e di quanto in esso contenuto, dipende dalla quantità e qualità del materiale in verifica e di comparazione.

Nel caso in cui l'esperto[4] sia chiamato ad esprimersi in un accertamento su firma elettronica priva dei dati biometrici, oppure a svolgere una verifica preliminare stragiudiziale su un documento firmato con tecnologia grafometrica, può avvalersi della rappresentazione grafica del file pdf (documento flat), indicando i limiti dell'accertamento, consapevole del fatto che nonostante l'immagine ottenuta possa essere fedele alla firma reale, non ne rappresenta l'esatta riproduzione.

E' opportuno in questi casi, che si possa disporre per la comparazione, di rappresentazioni grafiche generate dal medesimo tool forense (tablet-software) e nelle medesime condizioni (wifi o cavo).

4.2 In giudizio – Documento PDF FULL (definizione BPM ENFSI, versione 03, ottobre 2020)

Il documento full, che può essere messo a disposizione soltanto su autorizzazione dell' Autorità Giudiziaria (di seguito A.G.), permette all'Esperto di effettuare l'esame basandosi sui dati biometrici, sia attraverso una elaborazione qualitativa che quantitativa (statistico/matematica), e quindi di giungere a risultati più affidabili rispetto all'esame sul documento flat.

[4] Il termine è generico e comprende l'attività di C.T.U., Perito, C.T.o esperti delegati del Pubblico Ministero e C.T.P.

5. INCARICO

Con Ordinanza dell'A.G. procedente, il soggetto/i, il detentore/i del documento informatico contenente i dati biometrici della firma/e in verifica metterà a disposizione dell'esperto tali dati cifrati.

Una volta verbalizzata la presenza di tutti gli attori coinvolti vengono avviate le operazioni peritali con l'estrazione dei dati delle firme di interesse, che è necessario individuare nel caso in cui all'interno dello stesso file ci siano più firme apposte.

Nell'espletamento dell'incarico, l'esperto dovrà avere a disposizione un periodo analogo a quanto usualmente concesso per lo svolgimento di un accertamento su supporto cartaceo.

6. ESTRAZIONE DATI BIOMETRICI

6.1 Esibizione del file PDF

I documenti devono essere estratti dal sistema di conservazione a norma dell'Ente con evidenza che il documento fosse conservato correttamente. Dovranno essere riportati la data, la località di estrazione e le altre informazioni utili a garantire la tracciabilità del processo.

I documenti devono essere inviati dall'Ente al Giudice/Pubblico Ministero.

6.2 Numero firme da utilizzare

Non è possibile definire a priori il numero di firme necessarie per la comparazione.

E' opportuno disporre di un numero di scritture che coprano un ampio arco temporale e possibilmente:

- firme coeve alla datazione delle verificande;
- firme antecedenti e successive alla datazione delle verificande;
- saggio grafico.

Sono ammesse firme apposte su documenti cartacei.[5]

[5] E.N.F.S.I. – Best Practice Manual, Ed 03 ottobre 2020 Appendix 5.

6.3 Numero firme da utilizzare

I dati biometrici rilevati in fase di sottoscrizione, vengono inseriti all'interno del file secondo formati differenti a seconda della soluzione di firma utilizzata dall'Ente e fornita da un vendor di mercato.

Non esiste in Italia uno standard imposto a livello normativo. Ciò implica che questi dati siano leggibili e interpretabili solo dallo strumento forense dello stesso fornitore. Tuttavia esiste uno standard di riferimento sul tema della biometria ISO:19794-7:2014 applicabile anche alla grafometria. Nel citato standard vengono stabilite le strutture dati e la rappresentazione dei parametri biometrici che caratterizzano anche la sottoscrizione grafometrica.

6.4 Strumento forense

È necessario che l'Ente o l'esperto incaricato siano dotati di uno strumento forense (di seguito anche tool forense) della firma grafometrica. L'Ente avrà lo strumento forense dell'azienda che gli ha fornito la soluzione di firma, mentre l'esperto potrebbe avere lo stesso software o un altro di mercato. È opportuno che l'esperto sia dotato di un tool forense in grado di acquisire anche un file contenente le informazioni in formato ISO, in modo da poter lavorare sui dati biometrici estratti nei casi in cui il fornitore della soluzione di firma abbia implementato questo formato o abbia previsto una conversione dal suo formato proprietario. L'Ente può anche mettere a disposizione dell'esperto un elaboratore elettronico per l'espletamento dell'accertamento tecnico o, in alternativa, l'Ente fornisce all'esperto il software forense del proprio fornitore con la relativa licenza d'uso.

7. ATTIVITA' PERITALI

7.1 Sedi

Le attività avranno inizio in tribunale o presso una sede dell'Ente concordata con l'A.G.

7.2 Soggetti coinvolti

Sono coinvolti:

- l'ente, ovvero il detentore dei documenti informatici e dei correlati dati biometrici relativi alla firma/e grafometrica/e oggetto d'indagine;

- l'incaricato/i della conservazione della chiave privata di decifratura e/o delle credenziali di sblocco (Notaio o terza parte fiduciaria) incaricato dall'ente;
- l'esperto, qualora il software forense lo preveda, dovrà essere in possesso di strumenti inerenti la crittografia asimmetrica (token e smartcard) da utilizzare come cifratura dei dati biometrici estratti.

7.3 Verifica del file ed estrazione dei dati

La fase di verifica dell'integrità del file e l'estrazione dei dati biometrici deve avvenire su un elaboratore elettronico messo a disposizione dall'Ente o, qualora sia previsto dalla policy dell'Ente stesso, dall'incaricato alla conservazione della chiave di decifratura.
Per l'acquisizione da parte degli esperti incaricati dall'A.G. e dai Procuratori delle Parti, date le caratteristiche dei reperti in accertamento (dati grafometrici potenzialmente utilizzabili in modo fraudolento), si prospettano le seguenti modalità operative:

- Verifica che il file sia integro e che non sia stato corrotto dopo l'apposizione della firma. Questa verifica è fattibile con qualsiasi verificatore di documenti pdf, incluso Adobe. Tecnicamente una revisione dopo la firma, in linea con gli standard del formato pdf, può essere ritenuta valida in quanto è sempre possibile risalire alle modifiche effettuate;
- Estrazione dei dati biometrici;
- Decifratura dei dati biometrici utilizzando la chiave privata del certificato di cifratura utilizzato dall'ente (su dispositivo locale o su remoto HSM);
- Verifica che i dati biometrici inseriti dentro al documento pdf siano integri e che non siano stati alterati o corrotti dopo l'apposizione della firma. Questo controllo è fattibile solo con il software di estrazione dati del fornitore della soluzione di firma;
- Copia in chiaro nello strumento forense in mano all'esperto (vedi § 6.4);

Nel caso in cui lo strumento forense consenta una nuova cifratura dei dati biometrici, procedere con l'operazione, utilizzando lo strumento fornito dall'esperto.

Tutti i passaggi dovranno essere verbalizzati

8. PARTICOLARITA'

8.1 Esportazione file in formato ISO

Nel caso in cui l'esperto sia dotato di un suo strumento forense diverso da quello del fornitore dell'ente, ma in grado di importare file ISO, potrà procedere nel seguente modo:

a. obbligo di utilizzare il software fornito dal fornitore dell'ente per la verifica dell'integrità del file per l'estrazione e la verifica dei dati biometrici;
b. seguire la procedura di estrazione dati prevista dal fornitore;
c. convertire i dati in formato ISO;
d. aprire il software di analisi forense e importare i dati.

8.2 Esportazione file non in formato ISO

Nel caso in cui la firma sia stata apposta con soluzione non in grado di esportare file in formato ISO, l'esperto procederà nel seguente modo:

a. obbligo di utilizzare il software fornito dal produttore per la verifica e per l'estrazione dei dati;
b. seguire la procedura di estrazione dati prevista dal produttore;
c. eseguire l'accertamento utilizzando il software forense del produttore.

8.3 Log strumento forense

E' consigliabile che il software forense sia dotato di un log delle operazioni effettuate sia in fase di verifica sia in fase di successiva analisi.

8.4 Saggio grafico

Per eventuale acquisizione di uno o più saggi grafici per l'esame comparativo, l'operazione deve essere preliminarmente richiesta dall'esperto e autorizzata dall'A.G.

8.5 Cancellazione dati biometrici

Per quanto riguarda la cancellazione sicura dei dati biometrici acquisiti dalle parti in causa si rimanda alla normativa vigente del Provvedimento del Garante (All. A del 13 ottobre 2008 in materia di impiego di apparecchiature informatiche e successivi aggiornamenti).

A.G.I.
ASSOCIAZIONE GRAFOLOGICA ITALIANA

Presidente

Dott.ssa Eleonora GAUDENZI

Firmato da: GDNLNR72A64D612P/7420038101027982.OId04+OjVsIHaVZGEosk03HmPZ0=
Emesso da: ArubaPEC S.p.A. NG CA 2
Ora/data firma: 14-09-2022 10:38:40
Indirizzo IP: 87.17.133.217

POLIZIA SCIENTIFICA

Namirial

Amministratore Delegato

Dott. Massimiliano [illegible]

Signed by: [illegible] MASSIMILIANO
Issued by: Namirial CA Firma Qualificata
Signing time: 14-09-2022 10:40:10
IP address: 151.0.245.58

Direttore del Servizio Polizia Scientifica

Dott. Luigi Rinella

Firmato da: LUIGI RINELLA
Emesso da: TI Trust Technologies per il Ministero dell'Interno CA
Ora/data firma: 14-09-2022 10:54:28
Indirizzo IP: 212.14.140.2

ALLEGATO 1 – GLOSSARIO

AUTORITÀ' GIUDIZIARIA (A.G.): un complesso di organi istituzionali pubblici con funzioni giurisdizionali in campo civile, penale, costituzionale e amministrativo, composta da soggetti definiti "magistrati"
CTU: Consulente Tecnico d'Ufficio
CTP: Consulente Tecnico di Parte
CTPM: Consulente Tecnico del Pubblico Ministero
CERTIFICATO DIGITALE: Un certificato digitale è un documento elettronico che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto (una persona, una società, un computer, etc.) che dichiara di utilizzarla nell'ambito delle procedure di cifratura asimmetrica e/o autenticazione tramite firma digitale.
CHIAVE PRIVATA: V. crittografia asimmetrica
CHIAVE PUBBLICA: V. crittografia asimmetrica
CRITTOGRAFIA: La crittografia può essere definita un sistema che tramite l'utilizzo di un algoritmo matematico agisce su una sequenza di caratteri, trasformandola. Tale trasformazione si basa sul valore di una chiave segreta, ovvero il parametro dell'algoritmo di cifratura/decifratura. Proprio la segretezza di questa chiave rappresenta il sigillo di sicurezza di ogni sistema crittografico.
In base al genere di chiave utilizzato, è possibile suddividere in due tipologie questo sistema di cifratura informatica: quando è presente una chiave singola si parla di crittografia a chiave simmetrica o a chiave segreta (la chiave del mittente e quella del destinatario sono la stessa), quando invece vi sono due chiavi di cifratura distinte si parla di crittografia a chiave asimmetrica o a chiave pubblica (la chiave di cifratura è pubblica, mentre la chiave di decifratura è privata).
CRITTOGRAFIA ASIMMETRICA: la crittografia asimmetrica, conosciuta anche come crittografia a coppia di chiavi, crittografia a chiave pubblica/privata o anche solo crittografia a chiave pubblica, è un tipo di crittografia dove, come si evince dal nome, ad ogni attore coinvolto nella comunicazione è associata una coppia di chiavi:
• la chiave pubblica, che deve essere distribuita;
• la chiave privata, appunto personale e segreta, evitando così qualunque problema connesso alla necessità di uno scambio in modo sicuro dell'unica chiave utile alla cifratura/decifratura, necessità presente, invece, nella crittografia simmetrica.
Il meccanismo si basa sul fatto che, se con una delle due chiavi si cifra (o codifica) un messaggio, allora quest'ultimo sarà decifrato solo con l'altra. Ci sono due funzioni che possono essere realizzate: usare la chiave pubblica per autenticare un messaggio inviato dal titolare con la chiave privata abbinata; o cifrare messaggi con la chiave pubblica per garantire che solo il titolare della chiave privata possa decifrarlo.
In un sistema di crittografia a chiave pubblica, chiunque può cifrare un messaggio usando la chiave pubblica del destinatario, ma tale messaggio può essere decifrato solo con la chiave privata del destinatario. Per fare ciò, deve essere computazionalmente facile per un utente generare una coppia di chiavi pubblica e privata da utilizzare per cifrare e decifrare. La forza di un sistema di crittografia a chiave pubblica si basa sulla difficoltà di determinare la chiave privata corrispondente alla chiave pubblica. La sicurezza dipende quindi solo dal mantenere la chiave privata segreta, mentre la chiave pubblica può essere pubblicata senza compromettere la sicurezza.
DEVICE: Unità hardware (periferica/dispositivo elettronico); si dice in particolare di dispositivi e apparecchi ad alta tecnologia e di piccole dimensioni (smartphone, e-book reader, tablet PC ecc.), come:

- Signature PAD: periferica dedicata alla sola raccolta di dati;
- LCD Monitor: dispositivo video interfacciato via USB utilizzato DisplayLink, MCT o via HDMI;
- Tablet PC: PC con soluzione di raccolta dati integrata.

DATI BIOMETRICI: i dati biometrici sono, per loro natura, collegati all'individuo in modo diretto, univoco e generalmente stabile nel tempo, denotando la profonda relazione tra corpo, comportamento e identità della persona. Per questo motivo l'adozione di sistemi biometrici di raccolta dati e il relativo trattamento possono comportare rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato. Le caratteristiche prese in considerazione dal sistema di riconoscimento biometrico possono essere FISIOLOGICHE come le impronte digitali, l'altezza, il peso, il colore e la dimensione dell'iride, la retina, la

sagoma della mano, il palmo della mano, la vascolarizzazione, la forma dell'orecchio, la fisionomia del volto, e COMPORTAMENTALI, ossia azioni che normalmente l'individuo compie come l'impronta vocale, la manoscrittura, la firma, lo stile di battitura sulla tastiera, i movimenti del corpo.

DOCUMENTO INFORMATICO: il Codice dell'Amministrazione Digitale (CAD-DLgs 82/2005) definisce il documento informatico "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" in contrapposizione al documento analogico "rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti" e lo inquadra come elemento centrale di quel processo di innovazione della Pubblica amministrazione finalizzato alla completa digitalizzazione delle pratiche amministrative. Il documento informatico assume la caratteristica di immodificabilità se strutturato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione. Il documento informatico, identificato in modo univoco e persistente, è memorizzato in un sistema di gestione informatica dei documenti o di conservazione la cui tenuta può anche essere delegata a terzi.

ELABORATORE ELETTRONICO: macchina (o insieme di apparecchiature) destinata alla elaborazione dei dati secondo procedimenti definiti attraverso programmi svolti automaticamente dalla macchina stessa.

EMR: tecnologia a risonanza magnetica che consiste in uno strato di sensori presenti dietro lo schermo a cristalli liquidi (LCD) di un device. Ogni sensore è calibrato con precisione ed emette un debole segnale elettromagnetico. Questi segnali creano un campo magnetico che si estende di circa 5/10 mm (a seconda del device) oltre la superficie in vetro del dispositivo.

ENTE: azienda o ragione sociale che si è dotata della soluzione di firma grafometrica.

ESPERTO: Criminalista esperto in grafologia forense, specializzato in analisi e comparazione di firme biometriche. È necessario che l'esperto possegga oltre a conoscenze nell'ambito della perizia grafica anche conoscenza di teorie, tecniche analitiche e procedure applicabili all'analisi forense delle firme grafometriche e competenza nella valutazione delle evidenze emerse, comprovate da attestato di frequenza di corsi di specializzazione,

F.E. Firma Elettronica: Il regolamento eIDAS definisce la firma elettronica come "dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare". La firma elettronica appartiene solo alla persona fisica. Firmatario, pertanto, può essere solo una persona fisica mentre le persone giuridiche potranno avvalersi dei "sigilli elettronici".

F.E.A. Firma Elettronica Avanzata: Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che: consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario; creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati. È sostanzialmente una firma elettronica semplice, che presenta però alcune caratteristiche di sicurezza aggiuntive ed è inserita in un processo ben definito.

F.E.Q. Firma Elettronica Qualificata: La "firma elettronica qualificata", è una firma elettronica avanzata basata su un certificato qualificato per firme elettroniche: a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati; e) è creata con un "dispositivo per la creazione di una firma elettronica qualificata"; f) è basata su un "certificato qualificato per firme elettroniche".

FIRMA GRAFOMETRICA: si tratta di un processo di firma basato su tecnologia grafometrica. Prevede l'apposizione della firma autografa di un soggetto su un apposito device mediante il quale è possibile collegare al documento elettronico un insieme di dati biometrici che garantiscono la connessione univoca tra documento firmato e firmatario. Viene vergata a mano dal sottoscrittore su un apposito device per mezzo di una penna ottica. Attraverso tale specifico hardware nonché grazie ad un software a corredo, il sistema all'atto della sottoscrizione cattura tutta una serie di parametri biometrici relativi alla sottoscrizione che la rendono di fatto unica ed irriproducibile. I più comuni tra tali parametri sono le coordinate spaziali, la pressione, la velocità, l'accelerazione, i tratti in volo e gli stacchi (pen-up).

FORMATO ISO (International Organization for Standardization): le norme ISO sono numerate e hanno un formato del tipo ISO nnnn:yyyy – titolo, dove nnnn è il numero della norma, yyyy l'anno di pubblicazione, oltre al dal titolo dello standard. Il tracciato ISO 19747-7:2014 è quello relativo ai dati biometrici ed è utilizzato per "neutralizzare" i dati biometrici rispetto alle soluzioni di mercato.

FORNITORE: società che fornisce all'Ente la tecnologia di firma grafometrica.

FUNZIONE DI HASH: è la funzione che consente di ricavare (calcolare) l'impronta digitale di un file (digest) o, meglio, del suo contenuto, calcolare l'impronta significa cioè affidarsi ad una funzione logico- matematica che partendo da una sequenza di bit di qualsiasi "lunghezza" restituisca una sequenza di pochissimi caratteri alfanumerici, a lunghezza fissa e predeterminata. Ogni minima modifica del file o del testo produrrà una diversa stringa in uscita. La caratteristica fondamentale di queste funzioni è la loro difficile invertibilità, poiché, dato un valore di hash, è molto difficile risalire al messaggio originale.

HSM (Hardware Security Module): forniscono un ambiente a prova di manomissione e sottoposto ad hardening per un'elaborazione crittografica sicura, la generazione e la protezione di chiavi, la cifratura e molto altro ancora. Disponibili in tre fattori di forma certificati FIPS 140-2, gli HSM supportano un'ampia gamma di scenari di deployment.

MASTERKEY: certificato di cifratura dei dati biometrici. E' composta da una chiave pubblica (cifratura) e una chiave privata (decifratura). Viene generata da un Ente Terzo fiduciario.

PADES (Advanced Electronic Signature): si tratta di una firma elettronica che, basandosi sul formato PDF le modalità e le tecnologie per l'identificazione dell'autore del documento e per le informazioni contenute nel documento originale (secondo la norma ETSI TS 102 778 e lo standard ISO 32000-1), garantisce le qualità necessarie per essere definita "firma elettronica avanzata" (con valore legale) secondo quanto individuato dalla Direttiva 1999/93/EC . Secondo il CAD e secondo la Deliberazione dell'allora CNIPA n° 45 del 21/05/2009, il formato di firma PAdES, così come la firma CAdES e XAdES sono i tre formati consentiti per le firme elettroniche qualificate e digitali.

SMART CARD – TOKEN USB: dispositivi di firma utilizzati per la Firma Digitale e i servizi di identificazione, sono apparati elettronici in grado di conservare in maniera protetta le chiavi private e di generare al loro interno la Firma Digitale. Utilizzano microprocessori basati su standard previsti dalla legge, nei quali sono implementate avanzate tecnologie crittografiche in un ambiente con standard di sicurezza molto restrittivi.

STRUMENTO FORENSE: software applicativo sviluppato per procedere all'analisi dei dati biometrici relativi alla firma grafometrica.

ALLEGATO 2 – RIFERIMENTI NORMATIVI

CAD: (Codice dell'Amministrazione Digitale): D. Lgs 7 marzo 2005, n.82 e successive modificazioni.

eIDAS Eletronic Identification Authentication and Signature: Electronic Identification Authentication and Signature, Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno che abroga la direttiva 1999/93/CE; esso fissa norme e procedure comuni a tutti gli stati membri per i servizi fiduciari ed i mezzi di identificazione elettronica. eIDAS definisce regole comuni che garantiscono la piena interoperabilità a livello comunitario non solo per gli strumenti di firma elettronica certificata ma anche per l'identificazione web dei cittadini (SPID) e per i servizi di terza parte (ad es. sigilli elettronici, validazione temporale, servizio elettronico di recapito).

DPCM 22/02/2013 – Decreto del Presidente del Consiglio dei Ministri : "Regole tecniche in materia di generazione, apposizione e verifica delle firme informatiche avanzate, qualificate e digitali …" G.U. n. 117 del 21.05.2013.

Provvedimento del Garante del 12.11.2014 – Allegato A: "Linee-Guida in Materia di Riconoscimento biometrico e firma grafometrica".

ALLEGATO 3 – ISTRUZIONI DI UTILIZZO SOLUZIONE NAMIRIAL FORENSE NEI DIVERSI SCENARI

1. Firma apposta con soluzione firmagrafocerta di Namirial e masterkey emessa e conservata da Namirial TSP
    - Aprire il Namirial forense
    - Creare una nuova pratica
    - Selezionare il file da periziare
    - Procedere con le verifiche di integrità del documento
    - Selezionare la firma da periziare e procedere con l'estrazione dei dati biometrici all'interno dell'applicativo. Seguire la policy Namirial ITA per l'utilizzo della chiave di decifratura
    - Procedere con le verifiche di integrità dei dati biometrici
    - Importare la firma dentro al software

2. Firma apposta con soluzione firmagrafocerta di Namirial e masterkey emessa e conservata da terze parti
    - Aprire il Namirial forense
    - Creare una nuova pratica
    - Selezionare il file da periziare
    - Procedere con le verifiche di integrità del documento
    - Selezionare la firma da periziare e procedere con l'estrazione dei dati biometrici all'interno dell'applicativo. Seguire la policy dell'Ente emittente per l'utilizzo della chiave di decifratura
    - Procedere con le verifiche di integrità dei dati biometrici
    - Importare la firma dentro al software

1. Firma apposta con soluzione XYZMO di Namirial e masterkey emessa e conservata da Namirial TSP
    - Aprire il software Penanalyst
    - Selezionare il file da periziare
    - Procedere con le verifiche di integrità del documento
    - Selezionare la firma da periziare e procedere con l'estrazione dei dati biometrici all'interno dell'applicativo. Seguire la policy di Namirial TSP per l'utilizzo della chiave di decifratura
    - Procedere con le verifiche di integrità dei dati biometrici
    - Estrarre un file ISO per ogni firma
    - Importare la firma dentro Namirial forense (procedura manuale o automatica)

2. Firma apposta con soluzione XYZMO di Namirial e masterkey emessa e conservata da terze parti

- Aprire il software Penanalyst
- Selezionare il file da periziare
- Procedere con le verifiche di integrità del documento
- Selezionare la firma da periziare e procedere con l'estrazione dei dati biometrici all'interno dell'applicativo. Seguire la policy dell'Ente emittente per l'utilizzo della chiave di decifratura
- Procedere con le verifiche di integrità dei dati biometrici
- Estrarre un file ISO per ogni firma
- Importare la firma dentro Namirial forense (procedura manuale o automatica)

In tutti i casi, al termine del processo, salvare il file della perizia dove sono presenti le firme estratte o importate. E' necessaria la chiave pubblica del certificato di autenticazione dell'esperto che verrà utilizzata come chiave pubblica di cifratura.
Sul PC in utilizzo per l'estrazione dei dati, caricare la chiave pubblica installare (se non presenti) i driver necessari per accedere al token USB o alla smart card o la chiave pubblica estratti.

- procedere con l'importazione sul PC dell'esperto ed eseguire la prova di apertura utilizzando la chiave privata di decifratura presente nel dispositivo (token o Smart card);
- verbalizzare che i dati sono stati correttamente esportati e salvati in modo cifrato sul PC dell'esperto;

Se l'operazione è stata fatta direttamente nel PC dell'esperto, verbalizzare che i dati sono stati correttamente esportati e salvati in modo cifrato sul PC dell'esperto.