LE BUONE PRASSI

per

L'ANALISI FORENSE

di

FIRME GRAFOMETRICHE

Vers.1.7

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

Sommario

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

PREMESSA

La firma grafometrica è una modalità di firma elettronica realizzata con un gesto manuale del tutto analogo alla firma autografa su carta.

I dati di una firma si acquisiscono mediante un dispositivo in grado di acquisire dinamicamente il comportamento tenuto in fase di sottoscrizione. In funzione della tecnologia impiegata si possono ottenere diversi livelli di qualità: risoluzione posizionale, frequenza dei campioni nell'unità di tempo, disponibilità del dato relativo alla pressione dello stilo sulla superficie, inclinazione, ecc...

Essa viene inserita su un documento digitale con degli appositi dispositivi, eliminando definitivamente la carta e garantendo valore giuridico e probatorio al documento che s'intende sottoscrivere.

Il documento, firmato elettronicamente, è collegato alla registrazione del gesto di firma (vettore grafometrico) che viene cifrato con chiavi asimmetriche per consentire la sicurezza del dato biometrico raccolto.

Il documento viene inviato a un Conservatore di documenti elettronici, mentre la chiave privata per decifrare il vettore è custodita da un Terzo fiduciario che la metterà a disposizione esclusivamente su richiesta dell'Autorità giudiziaria per verificare l'integrità del documento elettronico e restituire il corrispondente vettore.

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

1) INTRODUZIONE

Questo documento è rivolto ai grafologi forensi esperti in analisi e comparazione delle firme grafometriche (da ora in poi GEFG) e presume che essi abbiano pregresse conoscenze specifiche della disciplina grafologica.

Esso spiega la metodologia da seguire a partire dall'acquisizione dei reperti fino alla presentazione delle prove in tribunale, pertanto il presente documento descrive i sistemi, le procedure, le risorse umane, le attrezzature e le strutture necessarie per l'analisi forense delle firme grafometriche.

Nel caso si renda necessario l'apporto di un ausiliario tecnico informatico, il grafologo forense ricorrerà a esperti operanti nel settore o qualificati da associazioni professionali esperti nella dematerializzazione dei documenti e delle archiviazioni.

2) GLI OPERATORI

Grafologo forense esperto in analisi e comparazione di firme grafometriche è il professionista che ha la responsabilità di condurre l'analisi attraverso l'esame scientifico e il confronto di firme grafometriche al fine di determinarne la provenienza.

Egli necessita di una formazione adeguata e continua, analoga a quella introdotta dall'Associazione Grafologica Italiana (A.G.I.) per i suoi soci ordinari grafologi forensi.

Egli è responsabile dell'analisi dei documenti, della valutazione dei dati raccolti, della stesura della relazione e della presentazione dei risultati.

È necessario che possegga conoscenza di teorie, tecniche analitiche e procedure applicabili all'analisi forense delle firme e anche competenza nella valutazione dei risultati ottenuti dall'analisi grafologica e grafometrica.

È altresì imprescindibile la conoscenza delle procedure del sistema giudiziario in cui svolge la professione.

2) STRUMENTI DELL'ESAMINATORE FORENSE

Sono tutti gli ausili necessari ad una osservazione minuziosa dei dati biometrici relativi alla firma/e e alla scrittura da esaminare, ovvero:

Hardware

1. P.C. dotato di programmi di gestione delle immagini e di misurazione dei parametri grafici;
2. tavoletta grafica;

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

Software:

1. per la criptazione e la decriptazione con procedura a "chiavi asimmetriche" dei dati biometrici relativi alla firma/e e alla scrittura;
2. per l'acquisizione, l'elaborazione, la trasmissione e la cancellazione sicura dei dati;
3. eventuali software e hardware per l'elaborazione del vettore biometrico qualora non sia disponibile in formato ISO (saranno forniti da chi di dovere).

3) LUOGHI DI LAVORO E CONDIZIONI AMBIENTALI

L'esame del dato biometrico avviene presso una postazione dedicata in *ambiente bianco* al fine di evitare la violazione dei dati biometrici.

4) TECNICHE, METODI E PROTOCOLLI DI ANALISI

Qualunque sia la natura del caso, il GEFG deve sempre utilizzare una combinazione di tecniche, fermo restando che la scelta della migliore metodologia deve essere effettuata durante la valutazione iniziale.

5) DOCUMENTAZIONE CASI ANALIZZATI

Ogni operazione compiuta dal GEFG deve essere dettagliatamente verbalizzata e contenere tutte le informazioni necessarie per permettere ad altri esaminatori di seguire il percorso svolto e valutare i risultati ottenuti.

Per le annotazioni si auspica che la verbalizzazione contenga:

1. il nome del soggetto detentore del file che contiene la firma grafometrica in verifica e di eventuali detentori delle firme di comparazione;
2. il nome del/i soggetto/i terzo/i fiduciario/ri detentore delle chiavi di decifratura dei dati biometrici relativi alla firma in verifica;
3. indicazione dell'HASH di identificazione dei file contenenti la firma grafometrica in verifica e le eventuali comparative, incluso il saggio grafico;
4. indicazione delle modalità di conservazione dei dati biometrici acquisiti, sia in verifica che in comparazione;
5. indicazione della modalità di acquisizione dei dati biometrici e di condivisione con le parti
6. indicazione della strumentazione e dei software adottati per l'acquisizione, elaborazione, conservazione e successiva eliminazione finale dei dati grafometrici

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

6) MODALITA' PROCEDURALI:

Successivamente alle disposizioni dell'A.G. procedente, il soggetto detentore dei file dei dati biometrici della firma grafometrica in verifica metterà a disposizione del perito tali dati cifrati.

In considerazione delle caratteristiche dei reperti in accertamento (dati grafometrici, potenzialmente utilizzabili in modo fraudolento) e presupponendo che – così come previsto dal Provvedimento generale in tema di biometria emanato dal Garante per il corretto trattamento dei dati personali il 12 novembre 2014 – i dati siano stati cifrati utilizzando una tecnica di cifratura basata su chiavi asimmetriche (una pubblica utilizzata per cifrare e una privata da utilizzare per decifrare), si propone di adottare la seguente modalità operativa:

1. Il GEFG invierà al detentore della chiave crittografica asimmetrica privata corrispondente a quella pubblica utilizzata per la cifratura dei dati biometrici (terzo fiduciario) una propria chiave asimmetrica pubblica.

   Il terzo fiduciario eseguirà la decriptazione del vettore biometrico cifrato, estrarrà lo stesso in chiaro e verificherà il suo collegamento con il contenuto originale (ad es. per mezzo di impronta HASH) comprovando così l'integrità del documento in esame.

2. Il terzo fiduciario provvederà a ri-cifrare i dati biometrici estratti con la chiave pubblica fornita dal GEFG.
3. Il terzo fiduciario fornirà (mediante un metodo che garantisca l'autenticità, es. con una pec o firmando digitalmente il messaggio o l'impronta HASH del vettore) al GEFG (perito, CTU o CT del PM) il vettore biometrico cifrato il GEFG decripterà con la sua chiave privata.
4. La condivisione dei dati della firma/e in verifica e di un eventuale saggio grafico con i CTP e le parti non può prescindere dall'esenzione dell'esperto incaricato dall'A.G. da ogni responsabilità del loro improprio utilizzo, in quanto ogni vettore biometrico è da considerarsi un originale;
5. Alla conclusione del procedimento è opportuno che venga prodotta all'A.G. l'attestazione della cancellazione sicura dei dati biometrici acquisiti dalle parti in causa: si consiglia l'utilizzo di una delle modalità di cancellazione previste dall'Allegato A) al provvedimento del Garante del 13 ottobre 2008 in materia di impiego di apparecchiature informatiche.

7) VERIFICA E STIMA DELL'INCERTEZZA DI MISURA

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.

Il GEFG può procedere anche all'esame delle firme *flat* che hanno un limitato valore giuridico in quanto non corredate da dati biometrici. In questo caso deve indicare i limiti dell'accertamento. L'errore umano si può arginare potenziando la formazione di base e continua dell'operatore, il quale è tenuto a seguire le linee guida indicate dalla comunità scientifica.

8) FORMAZIONE CONTINUA

Il GEFG sarà tenuto ad aggiornamenti specifici e continui, seguendo gli sviluppi della materia.

9) VALUTAZIONE INIZIALE

Tutto il materiale a disposizione deve essere valutato per determinarne l'idoneità. Devono essere tenute in considerazione le informazioni relative al caso ed eventuali carenze devono essere colmate, dove possibile, con il contributo del committente.

10) VALUTAZIONE DELLE IPOTESI

La valutazione dei dati raccolti con l'esame dei documenti deve comprendere la discriminazione di tutte le ipotesi formulate inizialmente e l'orientamento al giudizio che si è andato formando.

11) PRESENTAZIONE DELLE PROVE

Il GEFG, ove chiamato a esprimere il suo parere, deve attenersi ai principi etici del codice deontologico dell'Associazione di appartenenza, collaborando ai fini di giustizia con onestà, integrità, obiettività, scientificità e imparzialità.

12) PROVE SCRITTE: LA RELAZIONE

La relazione deve comprendere:

1. Numero di procedimento, committente e, nel caso intervenga, nome dell'ausiliario tecnico/laboratorio;
2. Qualifiche e firma del medesimo;
3. Data di assunzione dell'incarico e di consegna dell'elaborato;
4. Incarico e attività svolte dal consulente;
5. Metodo seguito e modalità procedurali;
6. Svolgimento dell'analisi;
7. Eventuali limiti intrinseci all'accertamento;
8. Risposta al quesito.

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

La relazione, al fine di oggettivare le tesi avanzate, conterrà tutto quanto utile a chiarimento dei concetti esposti.

13) PROVE ORALI: LA TESTIMONIANZA

Nel rendere testimonianza, il GEFG deve conoscere i principi procedurali che la governano e deve astenersi dal rispondere a domande che esulano dalla sua competenza, a meno che non sia specificatamente richiesto dall'autorità procedente.

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

APPENDICE 1

ELEMENTI FONDAMENTALI PER L'ANALISI PERITALE DELLE FIRME GRAFOMETRICHE

1) DOCUMENTI IN INDAGINE

Comprende tutte le analisi in grado di accertare la provenienza delle firme in verifica.

Nel caso di firme *flat* l'esperto è tenuto a specificare la tipologia del documento e a seguire le medesime modalità di analisi e comparazione di firma in copia cartacea prestando attenzione all'eventuale modifica dei parametri dimensionali.

2) CONOSCENZE RICHIESTE

È richiesta ai GEFG la conoscenza dei seguenti argomenti, ottenuta con un percorso di studi completo e documentato:

1. metodi operativi dell'esame forense delle firme
2. opportune conoscenze informatiche (hardware e software) per gestire un processo di analisi e comparazione di firme grafometriche
3. normativa civile e penale connessa alla specifica attività
4. normativa europea e italiana e sulle direttive del Garante della Privacy.
5. conoscenze delle varie tipologie di firma elettronica con o senza acquisizione di dati biometrici (firma elettronica semplice – firma elettronica avanzata – firma elettronica qualificata – firma digitale). D.Lgs 07.03.2005 nr. 82 Codice dell'Amministrazione Digitale.
6. conoscenze di base per gestire fogli di calcolo per l'elaborazione dei dati disponibili nel caso di firma grafometrica.
7. elementi di base in statistica descrittiva e inferenziale.
8. elementi di base dei sistemi di dematerializzazione dei documenti.
9. metodologie e tecniche crittografiche nell'ambito della codifica asimmetrica.

2) PRESUPPOSTI OPERATIVI

<u>Scrittura in verifica</u>

Nell'esame della scrittura in verifica occorre tenere presenti i seguenti presupposti:

1. tipologia delle tavolette grafiche (device) e dei relativi mezzi scrittori utilizzati;
2. stili grafici usati (stampatello/corsivo; tipologie di alfabeti diversi dal latino);
3. grado di identificabilità della scrittura secondo il quadrinomio della rarità, complessità, qualità della linea e velocità;

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

4. descrizione della firma ed eventuali variazioni;
5. accertamento del livello di fluidità/contrazione del tracciato sul tablet e livello di naturalezza /artificiosità della firma;
6. presenza e tipologia di eventuali dettagli grafici personalizzati e natura degli stessi.

Nelle scritture di comparazione occorre considerare i seguenti fattori:

1. età dello scrivente;
2. lateralizzazione;
3. livello grafico individuale;
4. livello di istruzione, professione;
5. malattie accertate o dichiarate, farmaci assunti aventi conseguenze sulla grafia;
6. eventuali dipendenze;
7. eventuali fattori stressanti.

Scritture di comparazione

Nelle scritture di comparazione occorre considerare fattori oggettivi come:

1. tipologia delle tavolette grafiche (device) e dei relativi mezzi scrittori utilizzati;

Saggio Grafico

Il saggio grafico deve essere strutturato conformemente ai reperti in analisi, possibilmente con mezzi grafici e supporti analoghi al reperto in indagine.

Nel saggio grafico occorre considerare:

2. naturalezza, spontaneità, dissimulazione della grafia;
3. modalità di redazione (postura, uso della mano opposta, etc.);
4. stili di scrittura per la valutazione dell'ambito di variabilità grafica;
5. campioni comparativi redatti con mezzi e su supporti di tipo differente;
6. omogeneità grafica con il rimanente materiale comparativo acquisito.

Per l'analisi autonoma delle comparative si rimanda all'appendice 3.

In fase di confronto occorre considerare i seguenti fattori:

1. similarità e differenze emerse;
2. compatibilità casuali;
3. valutazione delle stesse in termini di frequenza e rilevanza;

4. bilanciamento delle ipotesi di autografia/eterografia, in relazione alle ipotesi subordinate;
5. formulazione della risposta al quesito.

Grado della risposta peritale:

1. Attribuzione/non attribuzione;
2. Massimo grado di confidenza tecnica (è il livello più elevato di confidenza espresso dall'esperto il quale non ha riserve ed è certo, sulla base dell'evidenza analitica, che le firme a confronto abbiano/non abbiano la medesima origine);
3. Elevato grado di confidenza tecnica (l'evidenza del dato consente all'esperto di ritenere probabile che le firme a confronto abbiano/non abbiano la medesima origine);
4. Basso grado di confidenza tecnica (è il più basso livello di confidenza espresso dall'esperto al quale l'evidenza analitica suggerisce che le firme a confronto possano/non possano avere la medesima origine);
5. Impossibilità della risposta (è il punto zero della scala di confidenza. L'evidenza analitica non consente all'esperto di pervenire ad alcuna conclusione).

Ogni giudizio è da giustificare in base ad elementi obiettivi e alla letteratura peritale.

Tale scala di valutazione ha lo scopo di uniformare le modalità di espressione dei pareri richiesti agli operatori del settore.

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

APPENDICE 2

REQUISITI PER LA FORMAZIONE DEI GRAFOLOGI FORENSI ESPERTI IN ANALISI E COMPARAZIONE DI FIRME GRAFOMETRICHE

1) REQUISITI

Il GEFG, già in possesso dei requisiti previsti dall'A.G.I. per la qualifica di socio ordinario,

deve

1. aver frequentato un corso dedicato di almeno 160 ore che preveda formazione teorica e pratica;
2. essere iscritto negli albi del Tribunale di residenza e/o camera di commercio;
3. aggiornarsi periodicamente sulle tematiche inerenti per almeno 16 ore annue;

2) CORSO DI FORMAZIONE

Il corso di formazione dovrà prevedere i seguenti argomenti:

1. Conoscenza dei dispositivi hardware e degli applicativi software nella loro evoluzione;
2. Conoscenza teorica e pratica dei principali software di acquisizione, analisi ed elaborazione delle firme grafometriche;
3. Conoscenza delle procedure di estrazione, criptazione, decriptazione e cancellazione sicura del vettore biometrico ed elementi di crittografia asimmetrica;
4. Conoscenza delle varie tipologie di firme elettroniche (F.E.-F.E.A.-F.E.A.+C.Q.-F.E.Q.);
5. Conoscenza dettagliata di:
    I. Sicurezza della firma grafometrica;
    II. Certificazione della sicurezza nella firma grafometrica
    III. Interoperabilità degli standard ISO
6. Elementi di statistica descrittiva ed inferenziale;
7. Conoscenza delle principali suite per videoscrittura e fogli di calcolo;
8. Conoscenza delle norme privacy;

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

APPENDICE 3

PROCEDURE PER L'ANALISI E LA COMPARAZIONE DI FIRME GRAFOMETRICHE IN AMBITO FORENSE

1) INTRODUZIONE

Lo scopo dell'esame forense di una o più firme è di determinare se vi è o meno evidenza che esse abbiano una paternità comune.

L'approccio si basa su un esame oggettivo dei dati biometrici in ottica grafologica.

2) AMBITO DI APPLICAZIONE

Questa procedura riguarda l'esame e la comparazione di firme grafometriche con o senza dati biometrici (firma *flat*).

3) PRINCIPI

L'accertamento tecnico su firme, al fine di verificarne la provenienza da un determinato soggetto, si basa sui seguenti cinque postulati, accettati uniformemente dalla comunità scientifica internazionale ENFSI.

Ciascuno dei seguenti principi dipende dalla qualità e dalla quantità di scritture disponibili.

1. Non esistono due persone che firmano esattamente nello stesso modo;
2. nessuna persona firma esattamente nello stesso identico modo.
3. nella comparazione il valore di ciascuna caratteristica grafica, come prova di identità o di non-identità, dipende dalla sua frequenza, complessità, velocità relativa e naturalezza;
4. nessuno è in grado di imitare i caratteri della firma di un'altra persona mantenendo contemporaneamente la stessa velocità relativa e l'abilità grafica di chi sta cercando di imitare;
5. nei casi in cui chi scrive dissimula la propria firma abituale o imita la firma di un'altra persona, non sempre sarà possibile identificarne l'autore.

4) CONSERVAZIONE E GESTIONE DEI REPERTI

Tutti gli elementi di prova devono essere acquisiti, elaborati e conservati come previsto dalla normativa in vigore del Garante della Privacy. È necessario considerare il rischio di potenziale diffusione e contaminazione dei dati durante l'analisi (v.d. punto precedente LUOGHI DI LAVORO E CONDIZIONI AMBIENTALI)

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

5) PROCEDURE

Tale sessione fornisce una schematizzazione delle fasi analitiche del processo di analisi e comparazione di firme grafometriche in ambito forense

1. Preliminare verifica delle informazioni sull'integrità del vettore biometrico
2. esame autonomo della firma grafometrica in indagine;
3. analisi autonoma del materiale comparativo disponibile;
4. comparazione e determinazione degli elementi distintivi e valutazione dei dati emersi.

Le fasi di seguito indicate rappresentano norme che devono essere rispettate in ogni accertamento forense.

6) QUALITÀ E QUANTITÀ DEI REPERTI

1. discriminare se la firma è dotata di dati biometrici o priva (nel caso di firme *flat*, esporre eventuali limiti di accertamento);
2. potere identificativo della firma secondo la scala di seguito proposta:
    I. livello 0 = firma impersonale e non suscettibile di valutazioni (le modalità di esecuzione non permettono alcuna identificazione di mano).
    II. livello 1 = firma elementare, scolastica con poche informazioni.
    III. livello 2 = firma complessa.
    IV. livello 3 = firma altamente complessa.
3. anamnesi medica, storica e culturale (nazionalità) del soggetto ove possibile, entro i limiti di competenza;
4. eventuali circostanze, documentate o riferite dalle parti, che possono aver influenzato l'aspetto complessivo della firma;
5. valutare il materiale disponibile secondo i seguenti requisiti:
    I. comparabilità (omogeneità e qualità dei termini a confronto);
    II. adeguatezza (quantità);
    III. coevità.

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

6. determinare il tipo o lo stile di firma sottoposta ad analisi: descrizione oggettiva (stampatello, firme, sigla-firme, sigle).

7) CHECK LIST DEI LIVELLI ANALITICI

La check list è una guida volta alla verifica della/e firma/e al fine di uniformare gli accertamenti e consentire una rilevazione e verifica obiettiva dei dati emersi, sia per la/e firma/e in indagine che per quella/e in comparazione.

1. Format:
    i. Stile grafico della firma (firma, siglo-firma, sigla, firma leggibile/illeggibile etc.);
    ii. Collocazione spaziale della/e firma/e;
2. Dimensione della/e firma/e:
    i. Altezze relative e proporzioni interne;
    ii. Espansione verticale e orizzontale;
    iii. Spazio tra parole, tra lettere
3. Qualità esecutive;
4. Tempo di esecuzione;
5. Velocità (assoluta e relativa);
6. Continuità scritturale, movimenti aerei;
7. Inclinazione;
8. Allineamento di base;
9. Controllo della penna e del movimento (esitazioni, fluidità, tratti parassiti, tratti spuri, fenomenologia della stentatezza, fenomenologia della senescenza, etc.);
10. Qualità/modulazione dell'energia scritturale.
11. Morfografia:
12. Ideoformazioni;
13. elementi di dettaglio (segni grafici coattivi, rari e qualitativamente rilevanti);
14. Livello grafico;

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

15. complessità e personalizzazione rispetto al modello

8) CONFRONTO E BILANCIAMENTO DEI DATI EMERSI

Il confronto dovrà essere oggettivato attraverso l'esame incrociato di tutti i dati acquisiti autonomamente sul reperto in indagine e su quelli comparativi.

Nella fase del bilanciamento conclusivo, l'EGFG dovrà testare la resistenza delle ipotesi privilegiate rispetto alle contro ipotesi, al fine di verificare (seguendo un principio controfattuale) il peso probatorio dell'ipotesi conclusiva.

Per soddisfare i requisiti scientifici di tale resistenza l'esperto deve altresì verificare la correttezza dei seguenti parametri:

1. indici di immediatezza esecutiva;
2. completezza dei rilievi;
3. esattezza delle misure;
4. oggettività dei rilievi;
5. coerenza interna;
6. requisiti di omogeneità dei termini sottoposti a confronto;
7. corretta attribuzione dei valori "analogia" e "difformità";
8. corretta valutazione della complessità;
9. pertinenza delle argomentazioni ai dati analitici;
10. verifica del rapporto di coerenza-dati-valutazioni-giudizio.

9) FORMULAZIONE DELLE CONCLUSIONI

Le conclusioni espresse, metodologicamente così strutturate (confronta Appendice 1, grado della risposta peritale), sono in linea con le indicazioni provenienti da Scientific Working Group for Forensic Document Examination (SWGDOC), Guidelines for Forensic Document Examination, in Forensic Science Communications, aprile 2000 vol. 2 nr.2; Designation E1658-04 Standard Examiners, ASTM International; Scale of conclusions in collaborative exercises ENFHEX (European Network of Forensic Handwriting Expert).

10) EVENTUALE UTILIZZO DI COMPARATIVE CARTACEE

Nel caso si debbano utilizzare firme comparative su documenti cartacei (originali/copia) si farà riferimento a quanto prescritto nel protocollo "Le buone prassi per l'analisi forense della scrittura" pubblicato dall'Associazione Grafologica Italiana nel 2017.

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

FONTI NORMATIVE

- C.A.D.
- Regolamento UE 679/2016
- E.I.D.A.S. 910/2014
- Provvedimenti Ag.I.D.

GLOSSARIO

TERMINI, DEFINIZIONI, ACRONIMI

AGI

Associazione Grafologica Italiana è un'organizzazione senza scopo di lucro che da oltre 50 anni si occupa della divulgazione e dello sviluppo della disciplina grafologica e della qualificazione e aggiornamento dei grafologi professionisti ad essa aderenti, nei diversi ambiti di applicazione.

AgID

L'Agenzia per l'Italia Digitale (AgID) ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana (in coerenza con l'Agenda digitale europea) e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica.

AIFAG

Associazione Italiana Firma elettronica Avanzata Biometrica e Grafometrica, si pone l'obiettivo di promuovere e sostenere nel mercato delle firme l'adozione di standard sicuri e interoperabili e di stilare e fornire delle linee guida e delle "best practice" sull'utilizzo corretto della firma elettronica avanzata, biometrica e grafometrica.

ALGORITMO

In informatica, con il termine algoritmo si intende un metodo per la soluzione di un problema adatto a essere implementato sotto forma di programma. Un algoritmo si può definire come un procedimento che consente di ottenere un risultato atteso eseguendo, in un determinato ordine, un insieme di passi semplici corrispondenti ad azioni scelte solitamente da un insieme finito.

ANORC

Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale, iscritta nell'elenco del MISE, è un'associazione senza scopo di lucro che dal 2007 mette in comunicazione e canalizza le conoscenze e i bisogni di aziende, enti pubblici, professionisti ed esperti che operano con diversi ruoli nella Digitalizzazione e Conservazione digitale.

C.A.

Certification Authority è un soggetto terzo di fiducia (trusted third party), pubblico o privato, abilitato ad emettere un certificato digitale tramite una procedura di certificazione che segue standard internazionali e in conformità alla normativa europea e nazionale in materia.

C.A.D.

Il codice dell'amministrazione digitale (CAD) è un atto normativo della Repubblica Italiana, precisamente il decreto legislativo 7 marzo 2005, n. 82.

Esso costituisce un corpo organico di disposizioni che presiede all'uso dell'informatica come strumento privilegiato nei rapporti tra la pubblica amministrazione italiana e i cittadini dello Stato. Le norme più significative che contiene sono disposizioni sul documento informatico, la firma elettronica e la firma digitale.

CADES

La busta CAdES è un file con estensione .p7m, il cui contenuto è visualizzabile solo attraverso idonei software in grado di "sbustare" il documento sottoscritto. Tale formato permette di firmare qualsiasi tipo di file, ma presenta lo svantaggio di non consentire di visualizzare il documento oggetto della sottoscrizione in modo agevole. Infatti, è necessario utilizzare un'applicazione specifica.

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

Una chiave privata è una chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave privata è associata ad una chiave pubblica. Le chiavi private non devono essere scambiate né conosciute da nessuno che non sia il legittimo proprietario. Per maggiore sicurezza la maggior parte dei programmi memorizza su disco le chiavi private solo dopo averle cifrate con una password definita dall'utente.

CHIAVE PUBBLICA

Una chiave pubblica è una chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave pubblica è associata ad una chiave privata.

Le due chiavi sono, a priori, perfettamente interscambiabili, ma generalmente una delle due viene definita "pubblica" e una "privata" perché il poter distribuire una delle due è il principale vantaggio dei crittosistemi asimmetrici.

Le chiavi pubbliche possono essere scambiate anche su un canale non sicuro (via e-mail, tramite un key server, su una pagina web ecc.), l'importante è sapere che una chiave pubblica non è di per sé associata a una "persona", ma esclusivamente ad una chiave privata. Per associarla ad una persona si fa generalmente uso di un certificato digitale.

CIFRATURA ASIMMETRICA

Vedi 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 SIMMETRICA

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 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.

DEMATERIALIZZAZIONE

Con "dematerializzazione" si indica il progressivo incremento della gestione documentale informatizzata - all'interno delle strutture amministrative pubbliche e private - e la conseguente sostituzione dei supporti tradizionali della documentazione amministrativa in favore del documento informatico. La dematerializzazione si pone pertanto come un processo qualificante di efficienza e di trasparenza delle amministrazioni pubbliche, consentendo nel contempo grandi risparmi diretti in termini di carta e spazi recuperati, e indiretti in termini di tempo ed efficacia dell'azione amministrativa pubblica, delle aziende e dei privati.

DEVICE

Unità hardware; in particolare, 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.)

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 scrittura grafica, la firma, lo stile di battitura sulla tastiera, i movimenti del corpo.

DATI BIOMETRICI FIRMA ELETTRONICA

Coordinate spaziali X e Y, Velocità, Tempo e Pressione, Tratti in Volo.

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 formato 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

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

memorizzato in un sistema di gestione informatica dei documenti o di conservazione la cui tenuta può anche essere delegata a terzi.

EIDAS

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 e 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).

F.E.

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 soltanto una persona fisica. Le persone giuridiche potranno avvalersi dei "sigilli elettronici".

F.E.A.

La "firma elettronica avanzata", è una firma elettronica che soddisfa determinati requisiti. Questi requisiti sono indicati dall'articolo 26 del Regolamento: 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.

F.E.Q.

La "firma elettronica qualificata", è una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e 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".

ASSOCIAZIONE GRAFOLOGICA ITALIANA Corso Garibaldi 111 - 60121Ancona
ASSOCIAZIONE ITALIANA FIRMA ELETTRONICA AVANZATA BIOMETRICA E GRAFOMETRICA via Stampacchia, 21 - 73100 Lecce
ASSOCIAZIONE NAZIONALE PER OPERATORI E RESPONSABILI DELLA CONSERVAZIONE DIGITALE via Stampacchia, 21 - 73100 Lecce

FIRMA GRAFOMETRICA

La Firma Grafometrica è un processo di firma che prevede l'apposizione della firma autografa del cliente su un apposito tablet, mediante il quale è possibile "allegare" al documento elettronico un insieme di dati biometrici che garantiscono la connessione univoca tra documento firmato e firmatario. La firma grafometrica viene vergata a mano dal sottoscrittore su una apposita tavoletta elettronica a mezzo di una penna anch'essa elettronica. Attraverso tale specifico hardware nonché grazie ad un apposito 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. Il più comuni tra tali parametri sono la forma, la pressione, la velocità, l'accelerazione e i cosiddetti tratti in volo.

HASH

L'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, gestibile anche senza strumenti informatici (tanto da poterla trascrivere a penna anche su un banale foglio di carta). Esistono varie "tecniche" (algoritmi) per calcolare un'impronta come ad esempio il Secure Hash Algorithm 256 (SHA256) che genera un hash-digest (impronta) di 256 bit (apparentemente una sequenza di 64 caratteri che in realtà rappresentano i 256 Bit)

HSM

Gli HSM hardware security module forniscono un ambiente a prova di manomissione e sottoposto ad hardening per un'elaborazione crittografica sicura, la generazione e 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.

IMPRONTA

L'impronta digitale (in inglese finger print) del documento o HASH. Gli algoritmi di hash attualmente più usati sono: MD5 si tratta in questo caso di un condensato del documento che permette di verificare l'integrità di quest'ultimo); SHA (per Secure Hash Algorithm, che può essere tradotto con Algoritmo di tranciatura sicuro), crea delle impronte di una lunghezza di 160 bit SHA-1 è una versione migliorata di SHA del 1994 che produce un'impronta di 160 bit partendo da un messaggio di una lunghezza massima di 264 bit trattandolo per blocchi di 512 bit.

ISO

L'Organizzazione internazionale per la normazione (in inglese International Organization for Standardization), abbreviazione ISO, è la più importante organizzazione a livello mondiale per la

definizione di norme tecniche. I suoi membri sono gli organismi nazionali di standardizzazione di gran parte dei paesi del mondo (in Italia l'UNI, l'Ente italiano di standardizzazione). 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 e dal titolo dello standard.

MARCATURA TEMPORALE

La Marca Temporale è un servizio che permette di associare data e ora certe e legalmente valide ad un documento informatico, consentendo quindi di associare una validazione temporale opponibile a terzi. (cfr. Art. 20, comma 3 Codice dell'Amministrazione Digitale Dlgs 82/2005).

Il servizio di Marcatura Temporale può essere utilizzato anche su file non firmati digitalmente, garantendone una collocazione temporale certa e legalmente valida. Sui documenti informatici sui quali è stata apposta una Firma Digitale, la Marca Temporale attesta il preciso momento in cui il documento è stato creato, trasmesso o archiviato. Apporre una Marca Temporale ad un documento firmato digitalmente pertanto fa sì che la Firma Digitale risulti sempre e comunque valida anche nel caso in cui il relativo Certificato risulti scaduto, sospeso o revocato, purché la Marca sia stata apposta in un momento precedente alla scadenza, revoca o sospensione del Certificato di Firma stessa. Come sancito dall'articolo 49 del Dpcm del 30/03/2009, le Marche Temporali emesse devono essere conservate in appositi archivi per un periodo non inferiore a 20 anni.

L'apposizione di una Marca Temporale a un documento firmato digitalmente, quindi, ne garantisce la validità nel tempo.

MASTER KEY

VEDI CRITTOGRAFIA ASIMMETRICA.

PADES

PAdES è un acronimo che sta per PDF Advanced Electronic Signature. In buona sostanza si tratta di una firma elettronica che, basando 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.

RSA

L'algoritmo RSA, proposto nel 1978 da Rivest, Shamir e Adleman, da cui il nome, è il primo sistema di crittografia a chiavi pubbliche che sfrutta l'approccio di Diffie ed Hellman ed è anche quello attualmente più diffuso ed utilizzato. Può essere usato sia per cifrare sia per firmare

digitalmente documenti. È considerato sicuro se sono usate chiavi abbastanza lunghe (almeno1024 bit). La sua sicurezza si basa infatti sulla difficoltà di fattorizzare numeri interi molto grandi.

SHA

Vedi HASH. Nella Deliberazione n. 45 del 21 maggio 2009 del Cnipa, oggi Agenzia per l'Italia Digitale, contenente le regole tecniche per il riconoscimento e la verifica del documento informatico, viene indicato quale algoritmo da utilizzarsi ai fini della generazione e verifica della firma digitale per la sottoscrizione dei documenti informatici, il dedicated hash-function 4, corrispondente alla funzione SHA-256.

SIGILLO ELETTRONICO

Il sigillo elettronico serve per provare l'emissione di un documento elettronico da parte di una determinata persona giuridica, dando la certezza dell'origine e dell'integrità del documento stesso; oltretutto, secondo l'art. 35, ad un sigillo non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali solo perché è elettronico. Esistono due tipi di sigilli: sigillo elettronico avanzato e sigillo elettronico qualificato.

SMART CARD - TOKEN

Le Smart Card e i 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**.**

TEMPLATE

Insieme di caratteristiche numeriche derivate per estrazione, dal campione biometrico acquisito durante la fase di "enrollment" dell'utente (registrazione dell'utente). I template sono dati codificati ottenuti dalle "feature" uniche di una caratteristica biometrica. Dimensioni limitate favoriscono la cifratura e la memorizzazione su più supporti. Ad ogni riconoscimento vengono generati template diversi. Per ogni individuo sono (solitamente) memorizzati più template. I template vengono aggiornati periodicamente

RIFERIMENTI BIBLIOGRAFICI

Per la parte di competenza grafologica si rimanda alla bibliografia delle Buone prassi del grafologo forense.

Per quanto riguarda la parte riguardante il tema in oggetto:

-PLAMONDON, R. AND LORETTE, G. (1989). Automatic signature verification and writer identification - the state of the art. Pattern Recognition, 22(2):107 – 131.

-IMPEDOVO, D. AND PIRLO, G. (2008). Automatic signature verification: The state of the art. IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 38(5):609–635.

-IMPEDOVO, D., PIRLO, G., AND PLAMONDON, R. (2012). Handwritten signature verification: New advancements and open issues. In International Conference on Frontiers in Handwriting Recognition, (ICFHR), pages 367–372.

-HARRALSON H.H. & MILLER L., Developments in Handwriting and Signature Identification in the Digital Age, Routledge, 2012

-R. PLAMONDON, G. PIRLO, D. IMPEDOVO, “Online Signature Verification”, Handbook of Document Image Processing and Recognition, D. Doermann & K. Tombre (eds.), Springer, 2014, pp. 917-947.

Ulteriori testi e riviste di riferimento devono aver subito il vaglio della comunità scientifica (*peer review*) o comunque della commissione tecnica scientifica dell’ente che ha provveduto alla pubblicazione.