LE BUONE PRASSI

per L'ANALISI FORENSE

di FIRME GRAFOMETRICHE

Ottobre 2019

PREMESSA

Questo documento stilato nell'ottobre 2019, è rivolto ai grafologi forensi esperti in analisi e comparazione di firme grafometriche, che necessitano di conoscenze specifiche della disciplina grafologica forense. Contiene le procedure, le risorse umane, le attrezzature e le strutture necessarie per l'analisi forense delle firme grafometriche.

E' stato redatto in collaborazione con ANORC – Associazione Nazionale Operatori e Responsabili della Custodia di contenuti digitali.

INTRODUZIONE

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 rilevare dinamicamente il comportamento tenuto in fase di sottoscrizione. In funzione della tecnologia impiegata si possono ottenere informazioni relative ~~a~~: coordinate spaziali, frequenza dei campioni nell'unità di tempo, pressione dello stilo sulla superficie (tablet), inclinazione, ecc.).

Essa viene utilizzata su un documento digitale, eliminando definitivamente la carta e garantendo valore giuridico e probatorio al documento che s'intende sottoscrivere.

Il documento digitale viene associato ai dati biometrici (registrazione del gesto di firma) (vettore grafometrico) e cifrato con chiavi asimmetriche per consentire la sicurezza dei dati raccolti.

Il documento viene inviato ad un ente certificatore (C.A.), mentre la chiave privata è custodita da un Terzo fiduciario che la metterà a disposizione su esclusiva richiesta dell'Autorità Giudiziaria in caso di contenzioso.

- GLI OPERATORI

  Il Grafologo forense esperto in analisi e comparazione di firme grafometriche è il professionista che ha la il compito di verificare la paternità di una firma grafometrica, secondo i principi di oggettività e scientificità.

  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 l'Esperto possegga conoscenza di teorie, tecniche analitiche e procedure applicabili all'analisi forense delle firme grafometriche e competenza nella valutazione delle evidenze emerse.

  Viene inoltre richiesto all'Esperto la conoscenza delle procedure del sistema giudiziario in cui svolge la professione.

- STRUMENTI DELL'ESAMINATORE FORENSE

  Gli ausili necessari all'Esperto sono:

  Hardware
  - P.C. dotato di programmi di gestione delle immagini e di misurazione dei parametri grafici;
  - device;

Software:

- per la criptazione e la decriptazione con procedura a "chiavi asimmetriche" del documento informatico e dei dati biometrici relativi alla firma/e e alla scrittura;
- per l'acquisizione, l'elaborazione, la trasmissione e la cancellazione sicura dei dati;
- eventuali software e hardware per l'elaborazione del vettore biometrico qualora non sia disponibile in formato ISO – saranno comunque forniti.

- 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 del sistema informatico in uso e/o dei dati biometrici. Per *ambiente bianco* si intende una postazione di lavoro che sia dedicata esclusivamente all'acquisizione e all'analisi dei dati biometrici, privo di connessione in rete e con adeguate misure di sicurezza informatica e protezione dati. È previsto un backup dei dati, per salvaguardare la versione originale del dato, che potrebbe essere suscettibile a compromissioni.

- DOCUMENTAZIONE CASI ANALIZZATI

Ogni operazione compiuta dall'Esperto 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, in sintesi:

- il nome del soggetto/i detentore/i del documento informatico che contiene la firma grafometrica in verifica e di eventuali detentori delle firme grafometriche di comparazione;
- il nome del/i soggetto/i terzo/i fiduciario/i detentore delle chiavi di decifratura del documento informatico contenente i dati biometrici delle firme in verifica;
- indicazione dell'impronta HASH dei file contenenti la firma grafometrica in verifica e le eventuali comparative;
- indicazione della modalità di acquisizione dei dati biometrici da parte del CTU, del CTP e/o del Procuratore;
- la specifica di strumentazione e software adottati per l'acquisizione, elaborazione, conservazione e successiva cancellazione dei dati grafometrici, così come da normativa vigente e successive modifiche.

- MODALITA' PROCEDURALI:

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

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 per il Perito:

- IN PRESENZA:

  Alla fase di estrazione dei dati biometrici saranno presenti:

  - L'Esperto (Perito, CTU, o CT del PM) che dovrà essere in possesso, nonché certificato all'uso, degli strumenti inerenti la crittografia asimmetrica (Token e smartcard);
  - Il detentore dei documenti informatici e dei correlati dati biometrici relativi alla firma/e grafometrica/e oggetto d'indagine;

- Il C.T.P. o Procuratore che dovrà essere in possesso, nonché certificato all'uso, degli strumenti inerenti la crittografia asimmetrica (Token e smartcard);
- L'incaricato/i della conservazione della chiave di decifratura e/o delle credenziali di sblocco;
- Per il trasferimento dei dati biometrici relativi al saggio grafico, se preliminarmente autorizzato dall'A.G., il Perito incaricato seguirà la medesima procedura nei confronti dei CCTTPP o Procuratori. Atteso che ogni vettore biometrico è da considerarsi un originale, il Perito d'Ufficio declina ogni responsabilità del loro eventuale improprio utilizzo da parte dei CCTTPP o Procuratori.
- 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).

NB: Tutte le fasi descritte dovranno essere verbalizzate.

- TRAMITE PEC
  - L'Esperto (Perito, CTU, o CT del PM) invierà all' Ente terzo fiduciario incaricato della conservazione della chiave di decifratura la propria chiave asimmetrica pubblica.
  - Il Terzo fiduciario, verificata l'integrità del documento digitale (impronta di Hash) provvederà a ri-cifrare i dati biometrici e a trasferirli al Perito utilizzando la chiave pubblica fornita dallo stesso.
  - Il Terzo fiduciario invierà (mediante pec o e firmando digitalmente il messaggio, cioè il file) all'Esperto il vettore biometrico cifrato, il quale lo decripterà con la propria chiave privata.
  - Le modalità procedurali di cui ai punti precedenti riguarderanno anche i CCTTPP o i Procuratori.
  - Per il trasferimento dei dati biometrici relativi al saggio grafico, che dovrà essere autorizzato preliminarmente dall'A.G., l'Esperto incaricato seguirà la medesima procedura nei confronti dei CCTTPP o Procuratori.
    Atteso che ogni vettore biometrico è da considerarsi un originale, l'Esperto (Perito d'Ufficio) in questo modo declina ogni responsabilità del loro eventuale improprio utilizzo da parte dei CCTTPP o Procuratori.
  - Per quanto riguarda la cancellazione sicura dei dati biometrici acquisiti 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).

NB: Tutte le fasi descritte dovranno essere verbalizzate.

- FORMAZIONE CONTINUA

  L'Esperto sarà tenuto ad aggiornamenti specifici e continui.

- PRESENTAZIONE DELLE PROVE

  L'Esperto, ove chiamato a esprimere il suo parere, deve attenersi ai principi etici del codice deontologico dell'Associazione di appartenenza e secondo le norme vigenti.

- PROVE SCRITTE

  La relazione deve comprendere:

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

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

- PROVE ORALI: LA TESTIMONIANZA

  Nel rendere testimonianza, l'Esperto 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 specificamente richiesto dall'Autorità procedente.

APPENDICE 1

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

- REQUISITI

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

  deve

  - aver frequentato un corso dedicato di almeno 160 ore che preveda formazione teorica e pratica;
  - essere iscritto negli albi del Tribunale di residenza e/o camera di commercio;
  - aggiornarsi periodicamente sulle tematiche inerenti la materia con cadenza annuale;

- CORSO DI FORMAZIONE

  Il corso di formazione dovrà prevedere i seguenti argomenti:

  - Conoscenza dei dispositivi hardware e degli applicativi software nella loro evoluzione;
  - Conoscenza teorica e pratica dei principali software e hardware di acquisizione, analisi ed elaborazione delle firme grafometriche;

- Conoscenza delle procedure di estrazione, criptazione, decriptazione e cancellazione sicura del vettore biometrico ed elementi di crittografia asimmetrica;
- Conoscenza delle varie tipologie di firme elettroniche (F.E.-F.E.A.-F.E.A.+C.Q.- F.E.Q.);
- Conoscenza dettagliata di:
- Sicurezza della firma grafometrica;
- Interoperabilità dello standard ISO 19794/7
- Elementi di statistica descrittiva ed inferenziale;
- Conoscenza delle principali suite per videoscrittura e fogli di calcolo;
- Conoscenza delle norme privacy;

GLOSSARIO

TERMINI, DEFINIZIONI, ACRONIMI

A.G.I.

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.

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 Operatori e Responsabili della Custodia di contenuti digitali, 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
V. crittografia asimmetrica

CHIAVE PUBBLICA
V. crittografia asimmetrica

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 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.

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 manoscrittura, 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 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.

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 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".

FIRMA GRAFOMETRICA

La Firma Grafometrica è un processo di firma che prevede l'apposizione della firma autografa del cliente 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. La firma grafometrica viene vergata a mano dal sottoscrittore su una apposita device per mezzo di una penna ottica. 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 le coordinate spaziali, la pressione, la velocità, l'accelerazione, i tratti in volo e gli stacchi (penn-up).

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 DIGITALE

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 tracciatura 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 deriva il nome. E' 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