Manuale Operativo

Implementazione della Firmagrafometrica in un processo di Firma Elettronica Avanzata

Namirial S.p.A.
Via Caduti sul Lavoro n. 4, 60019 Senigallia (An) - Italia | Tel. +39 071 63494
www.namirial.com | amm.namirial@sicurezzapostale.it | P.IVA IT02046570426
C.F. e iscriz. al Reg. Impr. Ancona N. 02046570426 | REA N. AN - 157295
Codice destinatario T04ZHR3 | Capitale sociale € 7.586.766,90 i.v.

INDICE

1 INTRODUZIONE

1.1 SCOPO DEL DOCUMENTO E CAMPO DI APPLICAZIONE

Lo scopo del documento è la descrizione delle regole e delle procedure operative adottate dall'unità organizzativa di Sicurezza Informatica di Namirial per tutte le attività inerenti la gestione dei servizi di Firmagrafometrica inseriti in un processo di Firma Elettronica Avanzata (FEA).

Il documento è conforme con quanto qui sotto indicato:

- Titolo V (Firma Elettronica Avanzata) delle Regole Tecniche [X] in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, firme elettroniche qualificate, firme elettroniche digitali e validazione temporale dei documenti informatici, e nel Decreto Legislativo 30 dicembre 2010 [VIII], così come modificato dal Decreto Legislativo 7 marzo 2005 [III];
- conforme a quanto disposto dal provvedimento generale prescrittivo in tema di biometria del Garante per la protezione dei dati personali n. 513 del 12 novembre 2014, pubblicato sulla Gazzetta Ufficiale n. 280 del 2 dicembre 2014;
- conforme al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) [V].

Con frequenza non superiore all'anno, Namirial esegue un controllo di conformità della propria soluzione di Firmagrafometrica e, ove necessario, aggiorna questo documento anche in considerazione dell'evoluzione della normativa e standard tecnologici.

1.2 DEFINIZIONI ED ACRONIMI USATI ALL'INTERNO DEL DOCUMENTO

TERMINE	SIGNIFICATO
AES [Advanced Encryption Standard]	è un algoritmo di cifratura a blocchi a chiave simmetrica operante su un gruppo di bit di lunghezza finita.
Appartenenti all"Organizzazione	dipendenti e/o associati a favore dei quali l'Organizzazione richiede l'emissione di un certificato qualificato (Es. Aziende, Enti, Associazioni di categoria, ecc.)
AgID (ex DigitPA ex CNIPA)	Agenzia per Italia Digitale - D. Lgs. 22 giugno 2012 , n. 83, art. 22
Certificato digitale, Certificato qualificato	è un documento elettronico che attesta, con una firma digitale, l'associazione tra una chiave pubblica e l'identità di un soggetto (persona fisica). Art.28
Certificatore [Certification Authority - CA]	è l'ente, pubblico o privato, abilitato a rilasciare certificati digitali tramite procedura di certificazione che segue standard internazionali e conforme alla normativa italiana ed europea in materia.
Chiave privata	è la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave privata è associata ad una chiave pubblica, ed è solo in possesso dal Titolare che la utilizza per firmare digitalmente i documenti.
Chiave pubblica	è la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave pubblica è associata ad una chiave privata, ed è utilizzata per verificare la firma digitale apposta su un documento informatico dal Titolare della chiave asimmetrica.

CNIPA DigitPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione, l'Organismo di controllo istituito dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri.
Dispositivo Sicuro per la Creazione della Firma	dispositivo hardware capace di proteggere efficacemente la segretezza della chiave privata.
FEA	Firma Elettronica Avanzata
HASH	Funzione non invertibile che mappa una stringa di lunghezza arbitraria in una stinga di lunghezza predefinita. E' l'equivalente dell'impronta di un file in digitale, tradotta in una sequenza di bit.
Marca temporale [Timestamp]	è il riferimento temporale che consente la validazione temporale.
Manuale Operativo	è il documento pubblicato sul proprio sito internet che definisce le procedure applicate, le caratteristiche del sistema e le tecnologie utilizzate al fine da soddisfare l'articolo 56 comma 1 del [X].
Operatore	è la persona incaricata, dal Soggetto che eroga servizi di firma elettronica avanzata che identifica l'Utente; lo informa circa le condizioni d'uso della firma apposta e partecipa al processo di acquisizione della firma elettronica avanzata dell'Utente.
RSA	algoritmo di crittografia asimmetrica, basato su chiavi pubbliche e private.
SHA-1 [*Secure Hash Algorithm*]	Algoritmo di crittografia che genera un'impronta digitale di 160 bit.
SHA-256 [*Secure Hash Algorithm*]	Algoritmo di crittografia che genera un'impronta digitale di 256 bit.
Signature tablet	Dispositivo elettronico da connettersi ad un computer in grado di acquisire i dati biometrici di una firma autografa, I valori per il rilevamento dei biometrici sono: coordinate X-Y, pressione, tempo.
Soggetti che erogano servizi di firma elettronica avanzata	sono i soggetti giuridici che si avvalgono della firma elettronica avanzata al fine di utilizzarla nel processo di dematerializzazione dei rapporti intrattenuti con i propri Utenti e soggetti terzi (i propri clienti/utenti) per motivi istituzionali, societari o commerciali, realizzandole in proprio o anche avvalendosi di soluzioni realizzate dai soggetti che realizzano soluzioni di firma elettronica avanzata come indicato nel [X] articolo 55 lettera B).
Titolare	è la persona fisica, identificata dal Certificatore, cui è attribuita la firma digitale ed è stata consegnata la chiave privata del certificato stesso.
Utente	è il soggetto a favore del quale la Licenziataria mette a disposizione una soluzione di firma elettronica avanzata, per sottoscrivere i Documenti informatici

Tabella 1 - Definizioni ed Acronimi

2 FIRMA ELETTRONICA AVANZATA

2.1 FIRMA GRAFOMETRICA – SCOPO

La firma grafometrica viene utilizzata per la sottoscrizione di documenti. Si tratta di una modalità di firma che possiede requisiti giuridici e informatici grazie ai quali, se inserita all'interno di un determinato processo (vedi §1.10) ne consentono una qualificazione per legge come FEA. La normativa che regola questa materia è contenuta sia nel Decreto Legislativo n. 82/2005 (Codice dell'Amministrazione Digitale) sia nel DPCM del 22 febbraio 2013. I documenti che il Cliente sottoscrive con la firma grafometrica sono documenti informatici che:

- sul piano tecnico soddisfano i requisiti di sicurezza definiti dalla normativa vigente;

sul piano giuridico hanno lo stesso valore dei documenti cartacei sottoscritti con firma autografa

2.2 LIMITI D'USO

Il processo di firma elettronica avanzata (FEA) implementato in conformità con le disposizioni delle Regole Tecniche [X], è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto che eroga soluzioni di firma elettronica avanzata al fine di utilizzarle nel processo di dematerializzazione per motivi istituzionali, societari o commerciali.

La FEA ha l'efficacia prevista dall'articolo 2702 del Codice civile e integra il requisito della forma scritta (con alcune eccezioni: per gli atti di cui all'art. 1350, punti 1-12 codice civile, deve usarsi la firma digitale) e sarà fruibile da chiunque.

Quindi con la soluzione FirmaGrafoCerta possono essere gestiti tutti i documenti ad eccezione di quanto previsto dall'articolo 21 comma 2-bis, D.Lgs. 235/2010 [VII],

"Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale".

La firma elettronica avanzata non consente il libero scambio di documenti informatici: il suo uso è limitato al contesto.

2.3 QUANDO LA FIRMA GRAFOMETRICA È UNA FIRMA ELETTRONICA AVANZATA (FEA)

La tecnologia di Firma Grafometrica diventa una Firma Elettronica Avanzata se viene inserita in un processo conforme all'Art. 1 del CAD (modifiche ed integrazioni introdotte dal decreto legislativo 30 dicembre 2010, n. 235.) ed alle specifiche Regole Tecniche [X] (Art. 56) da questo previste, secondo cui la soluzione di Firma Elettronica Avanzata garantisce:

a) L'identificazione del firmatario del documento;
b) la connessione univoca della firma al firmatario;
c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
d) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
f) l'individuazione del soggetto di cui all'articolo 55, comma 2, lettera a) delle regole tecniche;
g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;
h) la connessione univoca della firma al documento sottoscritto.

2.4 OBBLIGHI A CARICO DEI SOGGETTI CHE EROGANO SOLUZIONI DI FIRMA ELETTRONICA AVANZATA

Nel DPCM 22 febbraio 2013 pubblicato nella Gazzetta Ufficiale del 21 maggio 2013 sono presenti degli articoli specifici alle regole tecniche per l'attuazione della Firma Elettronica Avanzata.

In particolare, l'Articolo 57 - Obblighi a carico dei soggetti che erogano soluzioni di firma elettronica avanzata – prevede i seguenti punti:

1. I soggetti di cui all'articolo 55, comma 2, lettera a) devono:

a) identificare in modo certo l'utente tramite un valido documento di riconoscimento, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;

DA FARE: In pratica la prima volta che si presenta la soluzione di firma grafometrica al cliente, questi dovrà essere informato tramite opportuna informativa e riconosciuto tramite l'acquisizione del documento di riconoscimento.
Va predisposta un'informativa in cui il cliente che firma dichiara di accettare che i suoi dati biometrici vengano gestiti con una FEA

b) conservare per almeno venti anni copia del documento di riconoscimento e la dichiarazione di cui alla lettera a) ed ogni altra informazione atta a dimostrare l'ottemperanza a quanto previsto all'articolo 56, comma 1, garantendone la disponibilità, integrità, leggibilità e autenticità;

DA FARE: Questo punto viene assicurato dai sistemi di gestione documentale a norma di legge che viene adottata nella propria gestione. E' specificato nell'Informativa.

c) fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui alla lettera b) al firmatario, su richiesta di questo;

DA FARE: Si può procedere con la stampa qualora ci sia una stampante disponibile nel caso di clienti che non hanno servizi internet attivi, con l'inserimento nell'area riservata dell'home banking per coloro che hanno servizi internet attivi. E' specificato nell'Informativa.

d) rendere note le modalità con cui effettuare la richiesta di cui al punto c), pubblicandole anche sul proprio sito internet;

e) rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dall'articolo 56, comma 1;

f) specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto,

g) pubblicare le caratteristiche di cui alle lettere e) ed f) sul proprio sito internet;

DA FARE: I 4 punti dal d) al g) devono essere implementati da chi utilizza la soluzione di firma grafometrica nei propri siti internet. Dovrà essere prevista una pagina sul proprio sito internet dedicato alla firma grafometrica con all'interno un documento come quello E' specificato nell'Informativa.

h) assicurare, ove possibile, la disponibilità di un servizio di revoca del consenso all'utilizzo della soluzione di firma elettronica avanzata e un servizio di assistenza.

DA FARE: va predisposta la revoca all'informativa da mettere sul sito internet o comunque da rendere disponibile al cliente che aderisce al servizio.

2.5 TUTELA ASSICURATIVA

Il soggetto che eroga soluzioni di firma elettronica avanzata, come indicato nelle Regole Tecniche [X] art. 57 com.2, si impegna a stipulare una polizza assicurativa, con società abilitata ad esercitare nel campo dei rischi industriali, per la copertura dei rischi dell'attività svolta e dei danni a tutela delle parti (Firmatari ed i Terzi) per almeno € 500.000 (cinquecentomila).

DA FARE: E' da capire bene il discorso della polizza a cosa si riferisce. L'inserimento di questa clausola serve a salvaguardare il mercato da soluzioni non affidabili. Infatti il soggetto di tipo a) deve pretendere che anche il soggetto di tipo b) sia coperto da un'assicurazione analogo a ancora più cautelativa. Voi avete la garanzia che, tra le altre sicurezze sul software, ha una polizza come Autorità di Certificazione che copre fino ad un massimale molto più elevato.

3 LA SOLUZIONE DI NAMIRIAL

3.1 PREMESSA

La tecnologia di Firmagrafometrica di Namirial, denominata FirmaGrafocerta, ha come prerogativa la presenza di un operatore di front-end (promotore, operatore di sportello, addetto ufficio etc…) che presiede all'atto della firmagrafometrica dell'utente e ne convalida la sua presenza.

Il processo soddisfa i requisiti di identificabilità dell'autore della firma, così come l'integrità e l'immodificabilità del documento informatico. Inoltre, la soluzione non prevede l'utilizzo di componenti terzi ma è interamente sotto il controllo di Namirial.

3.2 MODALITÀ DI FIRMA

La soluzione è proposta è la firmagrafometrica medium: l'operatore di front-end procede con il riconoscimento del firmatario, il firmatario firma su appositivo dispositivo. Il processo di firma viene chiuso con un certificato di firma tecnico client.

Il processo soddisfa i requisiti di identificabilità dell'autore della firma, così come l'integrità e l'immodificabilità del documento informatico. Inoltre, la soluzione non prevede l'utilizzo di componenti terzi ma è interamente sotto il controllo di Namirial.

3.3 VALUTAZIONE

Il Soggetto che implementa la soluzione di firmagrafometrica nella valutazione dell'implementazione di tale processo di firma, deve valutare i seguenti punti:

- la modalità di identificazione dell'operatore di front-end,
- la tipologia del documento sottoscritto,
- il valore giuridico,
- il numero di contenziosi sulla tipologia di documento,

- il rischio operativo,
- il rischio d'immagine.

3.4 COMPONENTI DELLA FIRMA GRAFOMETRICA

Il Sistema si compone di elementi hardware e software e di un processo di acquisizione di firma che è svolto dall'operatore di front-end, in conformità a quanto descritto nel presente documento.

3.4.1 SOFTWARE

Il software utilizzato è FirmaCerta Client o GraphoSign, realizzato da Namirial in Italia e conforme a:

AgID - DETERMINAZIONE N. 121/2019 Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate

AgID - DETERMINAZIONE N. 147/2019 Rettifica per errore materiale della determinazione n.121/2019

Il software FirmaCerta Client nella versione "firma qualificata" può essere scaricato gratuitamente sia dal sito del Certificatore Namirial www.firmacerta.it che presso il sito AgID www.agid.gov.it.a

Per poter utilizzare FirmaCerta con l'abilitazione alla firmagrafometrica occorre acquistare a parte il relativo modulo.

FirmaCerta Client è corredato di un SDK che consente una facile e rapida integrazione con applicativi nuovi e già esistenti.

3.4.2 HARDWARE

Gli hardware utilizzati possono essere signature tablet connessi ad un computer tramite un collegamento cifrato o tablet con schermo digitizer.

I dispositivi di acquisizione dei dati biometrici devono essere in grado di rilevare posizione (coordinate x,y dei punti), tempo e pressione della firma.

Sul sito www.firmagrafometrica.it nella sezione "dispositivi utilizzabili" sono segnalati i dispositivi certificati.

E' interesse di Namirial supportare il più vasto numero di dispositivi hardware in grado di rilevare i dati biometrici statici e dinamici del firmatario.

E' fondamentale per Namirial la garanzia della cifratura e decifratura dei dati scambiati (in particolare i parametri caratterizzanti la firma biometrica) con il sistema informativo del soggetto che eroga la soluzione secondo le differenti esigenze di processo.

La comunicazione tra Computer e Tavoletta avviene in modalità cifrata utilizzando l'algoritmo AES a 128 bit a doppia chiave simmetrica scambiata con algoritmo DIFFIE- HELLMAN. E' stato oggetto di accurata analisi la criticità legata alla possibilità di fare il dump della memoria a seguito del crash di una applicazione, ovvero una fotografia di tutto ciò che il processo ha allocato in memoria fino a quel momento tra cui anche i dati biometrici, se non opportunamente gestiti da software.

FirmaCerta Client utilizza un algoritmo che cifra i dati biometrici simultaneamente all'acquisizione non lasciando mai in memoria la totalità dei punti (comunicazione a blocchi).

3.4.3 CERTIFICATO DI PROTEZIONE DEI DATI BIOMETRICI SOFTWARE

La cifratura dei dati biometrici avviene attraverso un certificato di protezione dei dati biometrici emesso da Namirial in qualità di CA (di seguito denominata Masterkey). La chiave pubblica è rilasciata per ogni per ogni client, mentre la chiave privata, unica in grado di estrarre in chiaro i dati biometrici, è conservata da un ente terzo garante, che può essere Namirial in qualità di CA su dispositivo HSM, o in alternativa un Notaio/Studio Legale utilizzando dispositivi come ad esempio le Smart Card o Token USB (vedi Paragrafo 5).

L'ente terzo potrà essere chiamato in fase di contenzioso dall'autorità giudiziaria seguendo la policy prevista nelle condizioni generali di contratto della firma grafo metrica. Quindi, tale policy, inerente alla sicurezza del dato biometrico si rifà alle modalità di implementazione del software di gestione della firma descritte di seguito nel presente documento.

3.4.4 MARCATURA TEMPORALE

Namirial in qualità di CA dispone di un proprio servizio di Time Stamping Authority per l'erogazione di marche temporali conformi allo standard l'ISO 8601. Per rafforzare l'operazione di firma grafometrica è possibile apporre contestualmente ad ogni sottoscrizione una data certa.

La marca temporale o validazione temporale, è il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

Il tempo, a cui fanno riferimento le marche temporali di Firma Certa è riferito al Tempo Universale Coordinato, ed è costantemente aggiornato con INRIM (Istituto Nazionale di Ricerche Metereologiche) e con il sistema di posizionamento satellitare Navstar GPS (NAVigation Satellite Time And Ranging - Global Positioning System).

3.4.5 FUNZIONI DEL CLIENT DI FIRMACERTA

Le funzioni di maggior interesse di FirmaCerta Client sono:

- Firma di un qualunque documento informatico (documenti, immagini, programmi dati ecc.) nel formato CAdES.
- Firma di documenti PDF nel formato PAdES con apposizione di logo personalizzabile mantenendo il formato originale.
- Visualizzazione ed estrazione dei file firmati.
- Codifica dei file firmati in base64.
- Visualizzazione dei certificati contenuti nei dispositivi di firma.
- Verifica dello stato del dispositivo inserito.
- Cambio PIN del dispositivo di firma.
- Sblocco del dispositivo di firma.
- Visualizzazione del logo inserito nel dispositivo di firma (se installato).
- Verifica automatica delle firme apposte sui documenti (richiede connessione internet attiva).
- Verifica della validità della firma sulle CRL (richiede connessione internet attiva).
- Verifica della validità della firma per mezzo del servizio OCSP (richiede connessione internet attiva).
- Firma e Marcatura dei documenti digitali (richiede connessione internet attiva).
- Verifica in numero di Marche disponibili (richiede connessione internet attiva).
- Marcatura di firme elettronica avanzata (richiede connessione internet attiva).
- Controfirma.
- Marcatura Temporale nei formati CAdES-T, TSD, TSR e TST (richiede connessione internet attiva).

- Firma massiva di documenti (solo con dispositivi rilasciati da FirmaCerta).
- Acquisizione dei dati biometrici per l'apposizione della firma grafometrica
- Apposizione della firma grafometrica su documenti pdf da Tablet PC
- Verifica "forte" dell'integrità del documento e dei dati biometrici durante le operazioni di verifica delle firme.
- Verifica acquisizione della firma grafometrica.
- Cattura foto da WebCam ed inserimento nella firma.
- Creazione di campi firma alla fine del processo.

4 COME SI FIRMA IL DOCUMENTO DIGITALE

Il processo di firma è gestito su un file pdf e restituisce un file pdf con lo stesso nome, ma con l'aggiunta dei dati biometrici e dei dati di firma e, qualora attivata, di marcatura temporale.

Il file può essere firmato con operazione manuale passando per il software FirmaCerta o GraphoSign oppure può essere firmato in una soluzione integrata all'interno delle applicazioni. L'integrazione avviene tramite SDK con chiamate ad un eseguibile, passando determinati parametri e relative chiamate per i servizi di marcatura e di storage.

Il documento da firmare è visualizzato sul display del tablet signature, il *firmatario* mantenendo il controllo esclusivo del sistema di generazione di firma potrà:

a. prendere visione del documento eseguendo lo scroll dello stesso,
b. annullare l'operazione di firma,
c. cancellare la firma per riscriverla,
d. sottoscrivere il documento e premendo OK conferma la firma.

Durante la scrittura della firma sul display il tablet signature rileva i dati biometrici attraverso i quali, oltre alla possibilità di rappresentare il tratto grafico relativo alla firma, vengono memorizzate le principali grandezze comportamentali quali coordinate, pressione, tempo. La sicurezza del flusso dei dati biometrici rilevati dal dispositivo viene in una prima fase garantita dal sistema di sicurezza implementato dal produttore (cavo per tablet esterna, sistema operativo per tablet PC) e in una seconda fase dal software FirmaCerta che contestualmente all'apposizione del dato lo cifra in sicurezza e lo ingloba nel file pdf. L'atto della sottoscrizione viene completato con la generazione di file impronta (HASH) da utilizzare poi in fase di verifica e controllo.

Il documento emesso e sottoscritto è auto-consistente, contiene i dati biometrici crittografati che non possono essere estratti e apposti su altri documenti. La firma grafometrica non è alfanumerica ma riproduce esattamente la firma con la grafia personale del firmatario. Ogni singola firma ha una sua validità legale: è personale e a sistema la firma che viene apposta è trattata in vettoriale, mantiene quindi le caratteristiche di integrità e di qualità, con un'incidenza minima sull'aumento delle dimensioni del file.

Per i dettagli della modalità di cifratura è disponibile un documento tecnico di sicurezza riservato.

5 FIRMAGRAFOCERTA E I REQUISITI DELLA FEA

I requisiti che la firma elettronica avanzata devono garantire sono stabiliti dalle Regole Tecniche [X] Art. 56, comma 1 ed elencati nel paragrafo 5. Tali requisiti sono completamente soddisfatti dalla soluzione FirmaGrafoCerta.

In dettaglio:

VOCE	NAMIRIAL
a) l'identificazione del firmatario del documento;	Il firmatario va riconosciuto con la raccolta del documento d'identità o, più in generale, con le stesse modalità previste oggi per il cartaceo.
b) la connessione univoca della firma al firmatario;	E' nella natura della firma del titolare e, in particolare nel caso di GrafoCerta, viene assicurata dalla presenza e dalla qualità dello strumento grafometrico a supporto del perito. Se si adotta la soluzione STRONG l'identificazione e la connessione univoca sono rafforzate nel processo di FEA Namirial dall'apposizione contestuale della firma digitale di chi riconosce.
c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;	Nel caso della firma grafometrica, il sistema di generazione della firma viene considerato l'insieme Mano + Tablet + Dati biometrici. Il procedimento che avviene in un ambiente presidiato consente la verifica della certezza dei dati biometrici una volta apposti sul documento attraverso lo strumento grafometrico.
d) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;	Il processo GrafoCerta garantisce l'integrità del documento attraverso l'apposizione di una firma in formato PadEs con la contestuale generazione di HASH. E' possibile verificare che il documento non sia stato modificato ma anche che i dati biometrici (in caso di attacco informativo) non siano stati trafugati o corrotti.
e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;	La soluzione Namirial garantisce la possibilità di vedere sempre il documento in sottoscrizione in quanto, anche in casi di creazione ed esposizione di sintesi del documento (es: contabili), durante l'operazione di firma è possibile visualizzare a video l'originale. Le dimensioni del tablet utilizzato influenzano la capacità di visualizzare una porzione o l'intero documento. Il firmatario può ricevere una copia del documento sul cartaceo o eventualmente l'originale o copia di esso (versione flat del pdf) in formato digitale.
f) l'individuazione del soggetto di cui all"articolo 55, comma 2, lettera a)	L'Ente o l'azienda che propone la firma grafometrica dovrà essere soggetto proponente e rispettare tutti i requisiti previsti.
g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;	Il processo di FirmaGrafoCerta garantisce con la generazione degli HASH l'integrità del documento. Come ulteriore sicurezza su documenti pdf, l'Ente o l'azienda che propone la firma può generare documenti in formato PDF/A evitando quindi la presenza di macroistruzioni nei files.
h) la connessione univoca della firma al documento sottoscritto.	Il processo GrafoCerta lo consente attraverso la generazione di HASH al momento della firma, che vengono utilizzati poi in fase di verifica e controllo.

Tabella 2 - FirmagrafoCerta e i requisiti della FEA

6 INFORMATIVA ED ARCHIVIAZIONE DEI DOCUMENTI SOTTOSCRITTI

Le regole tecniche, Art. 57 comma 1, prevedono per il Soggetto che eroga servizi di firma l'obbligo di identificare in modo certo l'utente tramite un valido documento di riconoscimento, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione

dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente.

Al termine del processo di informativa bisogna conservare per almeno venti anni copia del documento di riconoscimento e la dichiarazione di cui alla lettera a) ed ogni altra informazione atta a dimostrare l'ottemperanza a quanto previsto all'articolo 56, comma 1, garantendone la disponibilità, integrità, leggibilità e autenticità.

E' fondamentale, ma non obbligatorio, quindi che il Soggetto che eroga servizi di firma si doti di uno strumento di conservazione digitale a norma di Legge dove archiviare quanto suddetto insieme al documento sottoscritto con firma grafometrica.

7 IMPLICAZIONI PRIVACY

L'adozione della firma grafometrica inserita in un processo di Firma Elettronica Avanzata, implica il trattamento dei dati biometrici. I suddetti dati biometrici non sono conosciuti da Namirial e neanche consultabili. Infatti, la cifratura viene effettuata con una chiave di protezione ad hoc che non consente la consultazione in chiaro degli stessi dati al soggetto che propone la soluzione; la chiave di decifratura viene conservata da un Ente terzo che viene coinvolto in fase di contenzioso per procedere con l'estrazione dei dati in chiaro.

Nello specifico la circostanza per la quale la firma grafometrica utilizza i dati biometrici del sottoscrittore imponeva, in corso di validità del Codice Privacy, l'applicazione dell'articolo 37, comma1, lettera a) della 196/2003 in merito all'obbligo di notifica al Garante. Si precisa che tali obblighi oggi, in vigente normativa Reg UE 679/2016 [V] sono venuti meno per cui il trattamento dei dati personali degli utilizzatori del servizio è lecitamente svolto in conformità al rapporto contrattuale richiesto dalle parti. Si sottolinea l'onere, in capo al soggetto titolare del trattamento di verificare, in osservanza al proprio dovere di accountability, la corretta ponderazione circa l'utilizzo della soluzione scelta

Art. 17 – Trattamento che presenta rischi specifici

Nel caso della soluzione di Firma Grafocerta offerta da Namirial S.p.A., si osserva che il trattamento dei dati biometrici avviene in modalità tali da gestire, allo stato dell'arte, i rischi specifici per i diritti e le libertà fondamentali e quanto altro prescritto nel sopra citato Art 14, nello specifico, in osservanza alla valutazione sui rischi effettuata internamente sul prodotto in oggetto e in conformità al concetto di accountability si rileva che il trattamento del dato biometrico, nei limiti sopra esposti, è strettamente legato e commisurato all'erogazione del servizio richiesto e che, in osservanza all'art 6 co. B risponde all'esigenza di fornire fedelmente un prodotto.

Art. 7 - Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.
2. L'interessato ha diritto di ottenere l'indicazione:
a. dell'origine dei dati personali;
b. delle finalità e modalità del trattamento

Non essendo chiaro a cosa ci si riferisce con forma intelligibile di un dato biometrico riferito alla firma grafometrica, Namirial S.p.A. garantisce la possibilità di salvare i dati in formato immagine statica o immagine animata.

OPERAZIONI PREVISTE DAL DPCM 22 febbraio 2013 (Regole Tecniche)

Nel DPCM 22 febbraio 2013 pubblicato nella Gazzetta Ufficiale del 21 maggio 2013 sono presenti degli articoli specifici alle regole tecniche per l'attuazione della Firma Elettronica Avanzata.

In particolare l'Articolo 57 - Obblighi a carico dei soggetti che erogano soluzioni di firma elettronica avanzata

– prevede i seguenti punti:

1 I soggetti di cui all'articolo 55, comma 2, lettera a) devono:

a) identificare in modo certo l'utente tramite un valido documento di riconoscimento, informarlo in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;

DA FARE: In pratica la prima volta che si presenta la soluzione di firma grafometrica al cliente, questi dovrà essere informato tramite opportuna informativa e riconosciuto tramite l'acquisizione del documento di riconoscimento.
E' stata predisposta l'informativa DICHIARAZIONE_ACCETTAZIONE_FEA da personalizzare nell'intestazione, in cui il cliente che firma dichiara di accettare che i suoi dati biometrici vengano gestiti con una FEA.
Namirial ritiene sia corretto e legale (supportata da legali esperti in materia) far sottoscrivere l'informativa con la grafometrica intesa come una firma elettronica semplice.
Namirial fornisce nativamente nel software la dichiarazione da compilare.

b) conservare per almeno venti anni copia del documento di riconoscimento e la dichiarazione di cui alla lettera a) ed ogni altra informazione atta a dimostrare l'ottemperanza a quanto previsto all'articolo 56, comma 1, garantendone la disponibilità, integrità, leggibilità e autenticità;

DA FARE: Questo punto viene assicurato dai sistemi di gestione documentale a norma di legge che viene adottata nella propria gestione. Specificato nel NOTA INFORMATIVA GRAFOMETRICA

c) fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui alla lettera b) al firmatario, su richiesta di questo;

DA FARE: Si può procedere con la stampa qualora ci sia una stampante disponibile nel caso di clienti che non hanno servizi internet attivi, con l'inserimento nell'area riservata dell'home banking per coloro che hanno servizi internet attivi. Specificato nel NOTA INFORMATIVA GRAFOMETRICA

d) rendere note le modalità con cui effettuare la richiesta di cui al punto c), pubblicandole anche sul proprio sito internet;
e) rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dall'articolo 56, comma 1;
f) specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto,
g) pubblicare le caratteristiche di cui alle lettere e) ed f) sul proprio sito internet;

DA FARE: I 4 punti dal d) al g) devono essere implementati da chi utilizza la soluzione di firma grafometrica nei propri siti internet. Dovrà essere prevista una pagina sul proprio sito internet dedicato alla firma grafometrica con all'interno un documento come quello NOTA INFORMATIVA GRAFOMETRICA

h) assicurare, ove possibile, la disponibilità di un servizio di revoca del consenso all'utilizzo della soluzione di firma elettronica avanzata e un servizio di assistenza.

DA FARE: è stata predisposta la revoca dall'informativa DICHIARAZIONE_REVOCA_FEA da personalizzare.

2. Al fine di proteggere i titolari della firma elettronica avanzata e i terzi da eventuali danni cagionati da inadeguate soluzioni tecniche, i soggetti di cui all'articolo 55, comma 2, lettera a), si dotano di una copertura assicurativa per la responsabilità civile rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali per un ammontare non inferiore ad euro cinquecentomila (500.000€).

L'assicurazione è un'estensione di una Responsabilità Civile che incide in modo minimale. Chi non ha la responsabilità civile la deve attivare.

3. Le modalità scelte per ottemperare a quanto disposto al comma 2 devono essere rese note ai soggetti interessati, pubblicandole anche sul proprio sito internet.

DA FARE: E' da capire bene il discorso della polizza a cosa si riferisce. L'inserimento di questa clausola serve a salvaguardare il mercato da soluzioni non affidabili. Infatti il soggetto di tipo a) deve pretendere che anche il soggetto di tipo b) sia coperto da un'assicurazione analogo a ancora più cautelativa. Voi avete la garanzia che, tra le altre sicurezze sul software, ha una polizza come Autorità di Certificazione che copre fino ad un massimale molto più elevato.
Una volta attivata l'assicurazione va dichiarata sul sito internet. Namirial ha predisposto l'inserimento dell'informazione sulla NOTA INFORMATIVA GRAFOMETRICA

In sintesi, se si intende implementare la soluzione di firmagrafometrica di Namirial all'interno di un processo FEA è necessario:

- riconoscere il firmatario acquisendo un documento di identità e fargli sottoscrivere l'informativa alla FEA qualora sia interessato;
- inserire sul proprio sito internet una sezione dedicata con dentro:
  - NOTA INFORMATIVA GRAFOMETRICA che contiene buona parte dei punti richiesti;
  - Facsimile della dichiarazione di revoca (DICHIARAZIONE_REVOCA_FEA);
- Un link che rinvia al sito www.firmagrafometrica.it dove sono presenti:
  - Condizioni Generali;
  - Il manuale operativo della firma grafometrica;
  - L"informativa privacy generica.

8 CONTENZIOSO

In caso di contenzioso sulla Firma Grafometrica, se inserita in un processo di Firma Elettronica Avanzata, è chi adotta la soluzione che deve dimostrare che la firma contestata è realmente della persona che lei indica. Quindi è lei che deve avviare la causa per smentire o confermare il disconoscimento.

Dovrete quindi fornire il documento originale in formato pdf, la versione contenente i dati biometrici blindati e cifrati, richiedendolo all'Ente che vi effettua la conservazione a norma di legge. Se si arriva al disconoscimento della firma grafometrica la procedura sarà la seguente:

- il giudice riceve il documento oggetto di contenzioso;
- convoca un grafologo in grado di utilizzare gli strumenti e la tecnologia.

A tal proposito Namirial ha avviato corsi di formazione con l'AGI (Associazione Grafologi Italiani) per creare una rete di professionisti esperti in materia;

- convoca l'Ente che conserva la chiave di decifratura dei dati biometrici (nella fattispecie Namirial) i cui riferimenti gli saranno stati forniti;
- il grafologo creerà un file perizia e procederà all'estrazione dei dati biometrici sui quali verrà effettuata la perizia grafologica in presenza delle parti.

In caso di convocazione di uno o più sospettati il grafologo farà apporre una o più firme e un saggio grafico per poter avere un elemento di confronto da utilizzare nella perizia.

RIFERIMENTI

NUMERO	DESCRIZIONE
[I]	Decreto Legislativo 4 aprile 2006 n. 159 Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale.
[II]	Decreto del Presidente del Consiglio dei Ministri 12 ottobre 2007 Differimento del termine che autorizza l'autodichiarazione circa la rispondenza ai requisiti di sicurezza di cui all'art. 13, comma 4, del DPCM, pubblicato sulla GU 30 ottobre 2003, n. 13
[III]	Decreto Legislativo 7 marzo 2005, n. 82 Codice dell'amministrazione digitale (e ss.mm.ii)
[IV]	Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 Il presente decreto ha abrogato il decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici. (GU n. 129 del 6-6-2009)
[V]	Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera

	circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
[VI]	Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
[VII]	Decreto Legislativo 30 dicembre 2010, n. 235 Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69. Codice dell'amministrazione digitale (pubblicato sulla Gazzetta Ufficiale n. 6 del 10 gennaio 2011)
[VIII]	Decreto Legislativo 22 giugno 2012, n. 83 Misure urgenti per le infrastrutture l'edilizia ed i trasporti. Art. 22. DigitPA e l'Agenzia per la diffusione delle tecnologie per l'innovazione sono soppressi. I due enti confluiscono nell'Agenzia per l'Italia Digitale
[IX]	Decreto Legislativo 17 dicembre 2012, n. 221 Misure urgenti per la crescita del Paese. Il CAD, modificato nell'articolo 21, afferma il principio secondo cui *"l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria."*. Questa modifica riporta la FEA ai metodi di disconoscimento classici del codice di procedura civile. (art. 214 del codice di procedura civile).
[X]	Regole Tecniche da DPCM 22 febbraio 2013 Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, firme elettroniche qualificate, firme elettroniche digitali e validazione temporale dei documenti informatici
[XI]	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

Tabella 3 - Riferimenti normativi

INDICE DELLE TABELLE