# FIRMA ELETTRONICA AVANZATA GRAFOMETRICA

# CONFORMITÀ ALLA NORMATIVA

## NAMIRIAL S.p.A.

SENIGALLIA – 07/01/2015

# PREMESSA

Il presente documento intende approfondire la posizione di NAMIRIAL S.p.A. in ambito normativo.
L'Ente erogatore è l'azienda o l'Organizzazione che decide di adottare la soluzione NAMIRIAL.

# LA SOLUZIONE NAMIRIAL

La soluzione tecnologica di Firma Grafometrica di NAMIRIAL S.p.A. denominata FirmaGrafoCerta, può essere considerata un processo di **Firma Elettronica Avanzata Autografa (FEA)**, se inserita in un flusso organizzativo corrispondente ai requisiti normativi conformi alle specifiche Regole Tecniche (DPCM 22 febbraio 2013).
Per il suo utilizzo peculiare, FirmaGrafoCerta opera con un certificatore accreditato per la firma qualificata (NAMIRIAL) e in presenza di un operatore di front-end (operatore di sportello, addetto ufficio, ecc…) che presiede all'atto della firma dell'utente.

Gli elementi disponibili nell'apposizione della sottoscrizione, sono i dati biometrici e comportamentali, quali: *Posizione della penna, Pressione, Tratto in aria* (percorso che fa la penna quando non tocca nel device, fino a 1cm ), *e Tempo. E' possibile elaborare velocità e accelerazione ai fini di analisi forensi.*
Nel caso di dispositivi Apple (e in futuro anche di altri) viene utilizzata una penna esterna che rileva la pressione. Il processo di raccolta dati, cifratura, inserimento nel documento in firma è stato realizzato per soddisfare i requisiti di identificabilità dell'autore della firma generata, così come l'integrità e la non modificabilità del documento informatico.
I dati biometrici vengono cifrati con una certificato definito "Masterkey" di cifratura. NAMIRIAL è in grado di generare la Masterkey (vedasi Policy 2014-10 FEA-Procedura_FirmaGrafometrica.pdf), può essere un certificato RSA sia 2048 sia 4096. La scelta sulla lunghezza della chiave è lasciata all'Ente erogatore.

I dati cifrati vengono successivamente inseriti nel pdf attraverso la creazione di una firma conforme allo standard europeo denominato PAdES.

Con la soluzione di FEA denominata FirmaGrafoCerta possono essere gestiti tutti i documenti, salvo quanto previsto dall'articolo 25 del Codice dell'amministrazione digitale, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, le quali, se fatte con documento informatico, devono essere sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale.

## SCENARI DISPONIBILI PER LA FEA

La soluzione viene proposta in tre modalità, utilizzabili contemporaneamente o separatamente a scelta, sulla base della tipologia dei documenti da sottoscrivere, dal loro valore giuridico e dal rischio di contestazioni. Il passaggio da una modalità all'altra è gestibile modificando delle opzioni negli strumenti di integrazione.

In tutti e 3 i casi può essere prevista l'apposizione di una firma qualificata da parte dell'Ente erogatore (firma automatica massiva), a conferma dell'avvenuta transazione (firma di chiusura).

In dettaglio:

***LIGHT***

L'operatore di front-end firma contestualmente all'utente con un certificato non qualificato rilasciato da NAMIRIAL CA all'Ente che eroga il servizio di FEA. Viene rilevato il solo tratto grafico del sottoscrittore.

***MEDIUM***

Analogamente alla Light, l'operatore di front-end firma contestualmente all'utente con un certificato non qualificato rilasciato da NAMIRIAL CA all'Ente che eroga il servizio di FEA. Vengono rilevati i dati biometrici e il tratto grafico del sottoscrittore.
E' una FEA a tutti gli effetti.


*Fig.1 - Schema Light e Medium*

***STRONG***

L'operatore di front-end firma contestualmente all'utente con un certificato qualificato , rilasciato da una Certification Authority accreditata presso DigitPA. Vengono rilevati i dati biometrici e il tratto grafico del sottoscrittore.


*Fig.2 - Schema Strong*

In sintesi, al processo MEDIUM viene aggiunto l'utilizzo di una Firma Qualificata che non è del soggetto che eroga il servizio di FEA ma dell'operatore e non è la firma di chiusura del documento. L'opzione STRONG è una peciliarità operativa di NAMIRIAL che non trova riscontro nella normativa di settore ma consente una maggiore sicurezza operativa rispetto alla MEDIUM.

Il passaggio da una MEDIUM ad una STRONG può avvenire in qualsiasi momento, semplicemente fornendo la firma digitale qualificata a chi effettua il riconoscimento.

A tutte e 3 le soluzioni possono essere aggiunti ulteriori elementi rafforzativi quali la geolocalizzazione dell'acquisizione della firma e/o l'acquisizione della foto del firmatario.

# CONFORMITA' ALLA NORMATIVA

## CONFORMITA' ALLA DEFINIZIONE DI FEA

La soluzione di firma elettronica avanzata di NAMIRIAL è pienamente conforme alle Regole Tecniche del DPCM del 22 febbraio 2013. La firma elettronica avanzata (FEA), normata al titolo V di tale Decreto, si caratterizza come un processo. Gli articoli relativi alla FEA (artt. da 55 a 60) sono osservati scrupolosamente con soluzioni tecniche innovative, e sono stati sottoposti a verifiche esterne per alcuni progetti già effettuati: Ispettori Banca D'Italia, Autorità per l'Energia, Agenzia Italiana del Farmaco e Garante Privacy. E' disponibile un team dedicato (interni ed esterni) che segue i rapporti con Agenzia Digitale per L'Italia, Garante della Privacy e le diverse Autorità dei vari settori.

**In dettaglio la soluzione garantisce pienamente i requisiti della FIRMA ELETTRONICA AVANZATA secondo quanto previsto dall'Art.56 delle Regole tecniche (DPCM 22 febbraio 2013) e prima ancora dall'Art. 1 del CAD:**

- l'identificazione dell'utente firmatario del documento;
- la connessione univoca della firma al firmatario;
- il controllo esclusivo da parte dell'utente firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici utilizzati per la generazione della firma;
- la possibilità di verificare in ogni momento che l'oggetto della sottoscrizione non abbia subito modifiche dopo l'apposizione della firma;
- la possibilità per l'utente firmatario di ottenere evidenza di quanto sottoscritto;
- l'individuazione del Soggetto che eroga servizi di firma elettronica avanzata;
- l'assenza di qualunque elemento nell'oggetto della sottoscrizione, idoneo a modificare gli atti, fatti o dati nello stesso rappresentati
- la connessione univoca della firma al documento sottoscritto.

## CONFORMITA' IN TEMA DI PRIVACY

La soluzione di firma elettronica avanzata di NAMIRIAL è pienamente conforme a quanto previsto nel recentissimo **Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014**.
Nel Provvedimento si stabilisce che alcune specifiche tipologie di trattamento possono evitare la verifica preliminare a condizione che vengano adottate tutte le misure e gli accorgimenti tecnici idonei a raggiungere gli obiettivi di sicurezza individuati con il Provvedimento. Devono essere altresì rispettati i presupposti di legittimità contenuti nel Codice e richiamati nel capitolo 4 delle linee-guida collegate al Provvedimento.

Nel paragrafo 4.4 del provvedimento è specificato che:

> *Il trattamento di dati biometrici costituiti da informazioni dinamiche associate all'apposizione a mano libera di una firma autografa avvalendosi di specifici dispositivi hardware è ammesso in assenza di verifica preliminare laddove si utilizzino sistemi di firma grafometrica posti a base di una soluzione di firma elettronica avanzata, così come definita dal D.lgs. n. 82/2005 (Codice dell'amministrazione digitale), che non prevedono la conservazione centralizzata di dati biometrici.*
>
> *L'utilizzo di tali sistemi, da un lato, si giustifica al fine di contrastare eventuali tentativi di frode e il fenomeno dei furti di identità e, dall'altro, ha lo scopo di rafforzare le garanzie di autenticità e integrità dei documenti informatici sottoscritti, anche in vista di eventuale contenzioso legato al disconoscimento della sottoscrizione apposta su atti e documenti di tipo negoziale in sede giudiziaria.*

La firma grafometrica è utilizzabile senza verifica preliminare solo per i sistemi di FEA. Questo perché l'impianto normativo contenuto nel DPCM 22 febbraio 2014 assicura con un ambiente di sicurezza per il trattamento del dato grafometrico (il Garante ha voluto mantenere alto il livello di sicurezza).

### ***4.4 Sottoscrizione di documenti informatici***

Il trattamento di dati biometrici costituiti da informazioni dinamiche associate all'apposizione a mano libera di una firma autografa avvalendosi di specifici dispositivi hardware è ammesso in assenza di verifica preliminare laddove si utilizzino sistemi di firma grafometrica posti a base di una soluzione di firma elettronica avanzata, così come definita dal Decreto Legislativo 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale" che non prevedono la conservazione centralizzata di dati biometrici.

L'utilizzo di tali sistemi, da un lato, si giustifica al fine di contrastare eventuali tentativi di frode e il fenomeno dei furti di identità e, dall'altro, ha lo scopo di rafforzare le garanzie di autenticità e integrità dei documenti informatici sottoscritti, anche in vista di eventuale contenzioso legato al disconoscimento della sottoscrizione apposta su atti e documenti di tipo negoziale in sede giudiziaria.

In tali casi, il presupposto di legittimità del trattamento dei dati biometrici è dato dal consenso, effettivamente libero degli interessati ovvero, in ambito pubblico, dal perseguimento delle finalità istituzionali del titolare. Il consenso è espresso dall'interessato all'atto di adesione al servizio di firma grafometrica e ha validità, fino alla sua eventuale revoca, per tutti i documenti da sottoscrivere.

Il titolare è esonerato dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni e limitazioni:

a) Il procedimento di firma deve essere abilitato previa identificazione del firmatario.

*Attività già prevista nell'articolo 57, comma 1, lettera a) del DPCM. Questo punto deve essere rispettato nello stesso istante in cui si dichiara di utilizzare una Firma Elettronica Avanzata (FEA); deve essere raccolto un documento di identità insieme all'adesione alla FEA, entrambi da conservare per 20 anni. Il punto è quindi già previsto – NAMIRIAL ha implementato flussi "standard" per l'identificazione che includono la raccolta documenti e la sottoscrizione dell'informativa FEA.*

*NAMIRIAL è in grado di offrire anche il servizio automatizzato all'interno di un work flow per la conservazione delle informative per 20 anni.*

b) Devono essere resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione di semplice utilizzo per l'interessato, che non comportino l'utilizzo di dati biometrici.

*La soluzione NAMIRIAL non sostituisce il cartaceo, bensì traduce 1:1 il processo in digitale ed e fruibile parallelamente al cartaceo, lasciano così nel piano rispetto delle regole tecniche la possibilità di far firmare il cliente con il cartaceo, in quanto non tutti sono obbligati ad aderire all'utilizzo della firma grafometrica.*

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

*NAMIRIAL ha da sempre fatto menzione alla caratteristica di cancellazione immediata dei dati biometrici una volta inseriti nel pdf. L'inserimento è istantaneo così come la cancellazione. Ad esempio, al contrario di altre soluzioni, non è possibile con NAMIRIAL cancellare firme singole su un documento in quanto questo implica la conservazione in memoria per un intervallo temporale. In caso di errori nella sottoscrizione le firme devono essere rieseguite dall'inizio.*

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

*NAMIRIAL è un certificatore accreditato AgID che emette certificati RSA 2048 – 4096. La chiave privata viene ad oggi gestita secondo opportuna policy in accordo con l'Azienda. Non ci sono problemi a consegnarla a soggetti terzi fiduciari che devono però essere attrezzati all'operazione.*

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

*Il dato biometrico non è mai trattato in chiaro. Le modalità di attuazione di questa prescrizione possono essere descritte nei documenti di cui alle lettere e) ed f) dell'articolo 57, comma del DPCM. NAMIRIAL propone e certifica solamente dispositivi che hanno caratteristiche in linea con quanto*

*previsto dal Garante. L'elenco dei dispositivi certificato è disponibile nell'apposita sezione del sito [www.firmagrafometrica.it](http://www.firmagrafometrica.it)*

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

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

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

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

*Risposta ai punti f, g, h ed i: La soluzione NAMIRIAL Firma Certa lavora esclusivamente sulla RAM e utilizza un algoritmo che cifra i dati biometrici simultaneamente all'acquisizione non lasciando mai in memoria la totalità dei punti (comunicazione a blocchi). I dati biometrici sono quindi protetti in tempo reale e non sono mai disponibili contemporaneamente in chiaro sui dispositivi. Inoltre sono inseriti immediatamente nel pdf senza possibilità di cancellazione se non eliminando il pdf firmato e riattivando un nuovo processo di firma sul documento originale. NAMIRIAL si rendo comunque disponibile ad effettuare penetration test in modalità black box a fine di collaudare l'infrastruttura*

j) L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, o da più soggetti, in caso di frazionamento della chiave stessa, e nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma e a seguito di richiesta dell'autorità giudiziaria. Le condizioni e le modalità di accesso alla firma grafometrica da parte del soggetto terzo di fiducia o da parte di tecnici qualificati sono dettagliate nell'informativa resa agli interessati e nella relazione di cui alla lettera k) del presente paragrafo, in conformità con quanto previsto all'art. 57, comma 1, lettere e) ed f) del d.P.C.M. 22 febbraio 2013.

*In sintesi il dato biometrico è disponibile solo per le perizie grafologiche nel caso di insorgenza di un contenzioso sull'autenticità della firma e a seguito dell'autorità giudiziaria. NAMIRIAL rispetta quanto richiesto dal Garante. Ha una policy per i casi di contenzioso e mette a disposizione degli strumenti grafologici tra i più avanzati. Gli strumenti forensi hanno ricevuto attestazione ufficiale da parte di A.G.I. (Associazione Grafologi Italiani).*
*NAMIRIAL nel documento tecnico di sicurezza dichiara:*
*In caso di contenzioso è possibile:*

1) *Verificare che il documento pdf non è stato modificato (e quindi corrotto) dopo l'apposizione della firma grafometrica (in tutti e 3 i casi) – questo è disponibile nativamente grazie alla creazione del campo firma standard PAdEs;*
2) *Verificare che i campi firma contengono i dati biometrici e che questi non sono stati corrotti (quindi che nessuno ha cercato di manometterli) – questo è fattibile solo utilizzando la chiave di decifratura.*

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

*I titolari dotati di certificazione del sistema di gestione per la sicurezza delle informazioni (SGSI) secondo la norma tecnica ISO/IEC 27001 e successive modificazioni che inseriscono il sistema biometrico nel campo di applicazione della certificazione sono esentati dall'obbligo di redigere la relazione di cui al precedente periodo, potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico. Dal testo si evince anche che la certificazione è applicata alle misure messe in atto dal titolare del trattamento. Quest'ultimo in generale non è dotato di certificazione 27001, mentre lo è il produttore o il system integrator. NAMIRIAL si rende disponibile ad fornire la consulenza necessaria alla realizzazione dell'apposita relazione tecnica.*