POLICY Firma Grafometrica - Ver. 2014.02 del 01.10.2014

POLICY

FIRMA ELETTRONICA AVANZATA

FIRMA GRAFOMETRICA

www.firmagrafometrica.it
www.sicurezzadigitale.net

1. Emissione certificato di cifratura (Master Key)

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) composto da:

- una parte pubblica che cifra;
- una parte privata che decifra.

Il certificato è personalizzato.
La chiave pubblica sarà installata:

- sul client in utilizzo nel caso di soluzione FORTE con firma remota (HSM) e nel caso di soluzione MEDIA (MEDIUM) (documentazione di sportello);
- sul dispositivo di firma qualificata per ogni operatore nel caso di soluzione FORTE (STRONG) con firma non remota (documentazione contrattuale);

La chiave privata, unica in grado di estrarre in chiaro i dati biometrici, sarà conservata da Namirial in qualità di ente terzo garante, essendo Namirial Certification Authority accreditata.

1.1. Certificato della Società terzo Namirial in qualità di CA

Se la scelta del soggetto che eroga soluzioni di firma elettronica avanzata (DPCM 22 febbraio 2013 - art. 55) si avvale del certificato emesso a nome di Namirial S.p.A., a tale soggetto sarà fornita la chiave pubblica di cifratura.
La chiave privata è mantenuta da Namirial S.p.A., che sarà chiamata in fase di contenzioso dall'autorità giudiziaria ed in presenza di un perito per attivare il processo di decifratura dei dati biometrici contenuti nel/nei documenti.

1.2. Certificato personalizzato della Società che eroga la firma

Il soggetto, nella fattispecie La Società, che eroga soluzioni di firma elettronica avanzata (DPCM 22 febbraio 2013 - art. 55) richiede un proprio certificato di cifratura, Namirial S.p.A. procederà alla generazione delle chiavi, alla conservazione dei dispositivi di decifratura ed alla consegna al Soggetto di una o più buste cieche (a seconda della copie generate) contenete le credenziali per attivare le operazioni di decifratura.
Questa modalità può essere richiesta solo da Enti Pubblici e Privati, Istituti Finanziari e grandi aziende previo verifica da parte di Namirial sulle modalità di conservazione della busta cieca (presso un Notaio, Studio Legale, o altro) ed il processo di richiesta delle stesse.

Il Soggetto che eroga il servizio di firma invia alla Namirial, compilando l'apposito modulo di richiesta (Mod.NAM CA15) allegato sub.A, i seguenti dati:

- **Ragione Sociale** (obbligatoria)
- **P.IVA o Cod.Fisc**ale (obbligatoria)
- **Durata del certificato** (di base 3 anni)

Namirial genera il certificato di cifratura con i seguenti dati:

CAMPO	DESCRIZIONE	NOTE
CN:	Firma GrafoCerta (FEA) **Pseudonimo società**	Identificativo tipo firma ed azienda cliente di Namirial; l'informazione è visualizzata nel sw FirmaCerta ed all'interno dei documenti PDF firmati.
O:	**Ragione sociale/P.IVA**	
Description:	Certificato di protezione	Utilizzato dal software di firma FirmaCerta
Validity:	**Validità certificato**	6 anni

La generazione e l'invio del certificato di firma attesta l'accettazione della richiesta rivolta dal Cliente a Namirial S.p.A.

La MasterKey può essere memorizzata in una o più Smart Card con certificazione di sicurezza Common Criteria EAL4+ e/o all'interno di un appliance HSM anch'esso con certificazione EAL4+. La MasterKey, al momento del rilascio, è sempre accompagnata dalle credenziali per l'utilizzo contenute in busta cieca. La MasterKey, all'interno di un dispositivo sicuro, è l'unica chiave in grado di decifrare i dati biometrici all'interno di un documento informatico.

La corretta custodia della MasterKey è di primaria importanza essenzialmente per due motivi:
- Per poter estrarre i dati biometrici nel caso si cui il documento deve essere sottoposto a perizia calligrafica su ordine del giudice.
- Per evitare l'uso fraudolento della stessa al fine di estrarre dati biometrici senza autorizzazione.

1.3. Generazione e custodia della MasterKey

La soluzione proposta per la generazione e la custodia della Masterkey.
Namirial genera la MasterKey memorizzandola su:
- 3 Smart Card
- HSM

Qualora La Società ne faccia esplicita richiesta, Namirial metterà a disposizione una seconda copia della MasterKey su HSM denominata *HSM_Collaudo.* Questa copia è destinata al collaudo dell'impianto di verifica del sistema di decifra eseguito una sola volta.

Smart Card
Le 3 (tre) Smart Card sono conservate dalla Certification Authority Namirial.
Una (1) Smart Card è conservata nella cassaforte del caveau della CA e due (2) Smart Card sono custodite presso la cassaforte del sito di Disaster Recovery.
Le Buste cieche con le credenziali delle tre Smart Card sono custodite presso la Società con

indicate le modalità per l'accesso alle stesse.

HSM

Una (1) copia della MasterKey è memorizzata sui due (2) HSM preposti del Certificatore. La chiave sarà soggetta a processi automatici di backup, nonostante sia conservata in modo di non essere estraibile o duplicabile.
Le Busta cieca con una prima **porzione delle credenziali** della MasterKey su HSM è custodita presso la Società con indicate le modalità per l'accesso alle stesse.
La seconda **porzione delle credenziali** della MasterKey su HSM è conservata, una copia presso la cassaforte del caveau della CA, la seconda copia presso la cassaforte del sito di Disaster Recovery.

HSM_Collaudo

Se richiesta, Namirial produce una (1) seconda copia della MasterKey su HSM. Detta copia ha associate credenziali diverse dalla precedente. Le credenziali **sono tutte contenute** in un'unica busta cieca consegnata alla Società. Namirial non garantisce il backup di questa chiave. Per questo motivo e per assicurare il massimo della sicurezza, il procedimento Namirial provvede automaticamente alla sua cancellazione dopo il suo primo e quindi unico utilizzo. Se richiesta la copia HSM_Collaudo, Namirial non si assume responsabilità derivanti dal mancato collaudo della procedura.

Controversie sulle firme

La Società e Namirial in qualsiasi caso di contenzioso tra la stessa Società e i Titolari delle firme, su domanda e modalità indicate dell'autorità giudiziaria, si devono rendere disponibili alle operazioni di decriptazione dei dati biometrici delle firme.

Aspetti di sicurezza

La Società è priva di una parte del processo di decifratura e non è in grado di alterare le firme dei propri clienti.
Namirial è priva di una parte del processo di decifratura e non dispone dei documenti firmati dai Clienti della Società.
E' fondamentale che La Società tenga separate le credenziali di sblocco conservandole in luoghi differenti, in modo da garantire la sicurezza e l'integrità dell'operazione di decifratura analogamente a come opera la CA nella conservazione dei dispositivi sicuri. La Società dovrà altresì comunicare i riferimenti degli incaricati alla conservazione.
E' altresì fondamentale ricordare che per i meccanismi di sicurezza adottati e per la configurazione degli HSM, Namirial non può in nessun modo recuperare le credenziali di sblocco o tentare in qualche modo l'estrazione delle chiavi.

2. Procedura per generazione del certificato di cifratura (Master Key)

La procedura per la generazione del certificato di cifratura ha le seguenti modalità:

1. Il Soggetto che eroga la soluzione di firma (regole tecniche art. 55 com. 2 let. a) fornisce, alla Certification Authority Namirial, i dati necessari alla generazione del certificato di cifratura come indicato al punto 1.2.

2. La Certification Authority Namirial presso il Caveau della CA, procederà alla generazione della Master Key e all'inserimento della stessa nei dispositivi,

3. Per ogni dispositivo contenente la Master Key è associata una busta cieca differente.

4. Alla cerimonia di generazione saranno presente, minimo, le seguenti figure:
    a. Responsabile, o suo incaricato, delle verifiche ed ispezioni (Audit) di Namirial;
    b. Responsabile, o suo incaricato, Registration Authority di Namirial;
    c. Responsabile, o suo incaricato, della Sicurezza di Namirial;
    d. Eventuale altra/e figura/e indicate dal Soggetto che eroga la soluzione di firma (facoltativo).

5. La presa in carico dei dispositivi contenenti la Master Key e le buste cieche avverrà in una delle seguenti modalità:
    a. Notaio, solo se richiesto dal Soggetto che eroga la soluzione di firma (regole tecniche art. 55) ovvero dalLa Società
    b. Referente dal Soggetto che eroga la soluzione di firma (regole tecniche art. 55)

6. Verbali interni Namirial:
    a. cerimonia di emissione (key ceremony);
    b. custodia dei dispositivi e della porzione di credenziali;
    c. consegna delle credenziali al Soggetto che eroga la soluzione di firma;

3. Emissione certificato di firma tecnico MEDIUM

Il certificato di firma digitale emesso dalla Certification Authority di Namirial S.p.A. è fornito come file da installare sui computer degli operatori di Front-End.
Il certificato può essere emesso per ogni operatore, per ogni filiale, per ogni area, per ogni Società.

La Società che eroga il servizio di firma invia alla Namirial, compilando l'apposito modulo di richiesta (Mod.NAM CA16) allegato sub B, i seguenti dati:

- **Pseudonimo** (obbligatorio)
- **Ragione Sociale** (obbligatoria)
- **P.IVA o Cod.Fiscale** (obbligatoria)
- **Tipo di certificato nominale o societario** (obbligatorio)
    - **Nominale: Codice fiscale, Cognome e Nome** se nominale (facoltativi)
    - **Societario: unità organizzativa** (facoltativo)

Namirial genera il certificato di firma tecnica (MEDIUM) con i seguenti dati:

CAMPO	DESCRIZIONE	NOTE
CN:	Firma GrafoCerta (FEA) **Pseudonimo**	Identificativo tipo firma ed azienda cliente di Namirial; l'informazione è visualizzata nel sw FirmaCerta ed all'interno dei documenti PDF firmati.
O**:**	**Ragione sociale/P.IVA**	
OU:	**Unità organizzativa** o **Cod.Fisc/Cognome Nome**	(opzionale)
Description**:**	Firma Grafometrica	Utilizzato dal software di firma FirmaCerta
Validity:	Validità certificato	6 anni

La generazione e l'invio del certificato di firma attesta l'accettazione della richiesta rivolta dal Cliente a Namirial S.p.A.

4. Tool forense – modalità di gestione busta cieca e "Master key"

Il Tool forense è il software fornito da Namirial S.p.A. per l'analisi forense dei dati biometrici contenuti in un documento informatico prodotto dal client FirmaCerta.

L'analisi dei dati biometrici è svolta, in genere, da un Perito Calligrafo (CTU) nominato dal Giudice.
Il Perito per poter svolgere l'attività deve poter disporre:

- del/dei documento/documenti soggetti a perizia;
- del Tool forense di Namirial S.p.A.;
- della Master Key e della busta cieca custodite sulla base dello scenario di conservazione prescelto, tra quelli indicati;

Il Perito che utilizza il software Namirial dovrà essere in possesso di un proprio dispositivo sicuro contenente sia il certificato di firma che il certificato di autenticazione o un certificato CNS, per cifrare tali dati. Queste quantità di sicurezza sono fornite da Certification Authority di Namirial.

Linee guida del processo peritale
Le line guida non sono esaustive, descrivono un'ipotesi formulata dai periti sulla loro esperienza attuale; alcuni passaggi del processo sono a discrezione del Giudice.

1. Il Perito Calligrafo (CTU) è nominato dal Giudice.
2. Il Giudice o La Società consegnerà copia dei documenti al CTU con apposito verbale.
3. Il CTU dovrà essere formato sull'utilizzo dello strumento. Potrà avere la sua licenza o, inc aso contrario, potrà richiedere alLa Società di mettere a disposizione una postazione con il Tool Forense di Namirial S.p.A. e Signature Tablet. La Società e i l CTU potranno concordare se La Società fornirà un computer con installato il Tool Forense o fornirà solo la licenza dello strumento.
4. Il soggetto incaricato della conservazione delle credenziali per lo sblocco della chiave privata di decifratura si recherà nel luogo preventivamente concordato, con la busta cieca e con il dispositivo contenete la "Master Key";
5. Se è la prima perizia, dopo che il dispositivo sarà inserito nell'apposito lettore, il CTU aprirà la busta cieca e digiterà il PIN.
6. Il CTU estrarrà i dati biometrici dai documenti con il sussidio del Tool Forense.
7. Il soggetto incaricato della conservazione estrarrà dal lettore il dispositivo contenete la "Master Key", e ne manterrà il controllo fisico.
8. Il Perito, in possesso di un proprio dispositivo sicuro contenete sia il certificato di firma che di autenticazione (o in alternativa un certificato CNS), lo inserirà nel lettore, digiterà il PIN di sblocco e procederà al salvataggio cifrato dei dati biometrici.
9. Il CTU verificherà che l'operazione sia andata a buon fine, e che sia in grado di leggere i dati salvati.

10. Il soggetto incaricato della conservazione, se lo riterrà opportuno, cambierà il PIN di accesso al dispositivo contenete la “Master Key”, utilizzando il software FirmaCerta.
11. Il soggetto incaricato della conservazione inserirà in busta chiusa il PIN e conserverà la busta ed il dispositivo contenete la “Master Key”.
12. Il soggetto incaricato della conservazione redigerà apposito verbale, concludendo la sua attività.