Sicurezza Informatica

SIAV S.P.A.

nei

Firma Digitale, Firma Grafometrica

Trattazione degli aspetti tecnologici, il loro valore legale, i benefici del loro utilizzo, l'uso pratico

Namirial
SICUREZZA INFORMATICA

Udine, 06 dicembre 2013

Namirial SpA

ANORC gold

- **Premessa**
- **Le Firma informatiche**
- **La Firma Digitale**
- **La Marca Temporale**
- **La Firma Elettronica Avanzata Grafometrica**
- **La Posta Elettronica Certificata**
- **Validità europea e regolamenti futuri**

Chi è Namirial

Società di software e servizi per Enti, CAF, Banche, professionisti ed aziende.

- **Ente Certificatore** accreditato nel 2010 presso DigitPA (ex CNIPA - Centro Nazionale dell'Informatica per le Pubbliche Amministrazioni) ed autorizzato all'emissione di **certificati qualificati** conformi alla Direttiva europea 1999/93/CE, **certificati CNS** e **marche temporali**.
- **Gestore di PEC**, dal 26/02/2007, accreditato presso DigitPA (ex CNIPA - Centro Nazionale dell'Informatica per le Pubbliche Amministrazioni) ed autorizzato alla gestione di caselle e domini di Posta Elettronica Certificata.
- **Certificata UNI EN ISO 9001:2008**. Namirial ha conseguito il certificato n. 223776 rilasciata da Bureau Veritas Italia S.p.A.
- **Certificata UNI EN ISO 27001:2005**. Namirial ha conseguito il certificato n. IND12.2513U rilasciata da Bureau Veritas Italia S.p.A.

I numeri di Namirial

Società al 100% capitale italiano con 7 sedi in Italia:

Sede principale/legale: Senigallia (AN)

Sedi operative:
Ancona (AN)
Azzano Decimo (PN)
Casalnuovo (NA)
Gallarate (VA)
Modica (RG)
Reggio Emilia (RE)

Fatturato 2012: 14,60 Mil. €
Dipendenti: 162
Oltre 52.000 clienti soddisfatti
Oltre 290.000 PEC attivate
Oltre 5.000.000 di dichiarazioni dei redditi elaborate con i propri software

La dematerializzazione → ecologia digitale

Namirial S.p.A. orienta il proprio business sul concetto di innovazione ed ecologia digitale, ovvero la revisione delle procedure per **la sottoscrizione autentica**, **l'invio** e **la gestione dei documenti** in ottica informatica. Il risultato è una presenza sempre maggiore nei tre distinti settori del concetto di ecologia digitale strettamente collegati tra loro.

Fasi operative

Creare	*Comunicare*	*Gestire*
Firma digitale, firma grafometrica marcatura temporale.	**Posta Elettronica Certificata**	**Scansione, Gestione Documentale ed Archiviazione Sostitutiva**

5

- Premessa
- **Le Firma informatiche**
- La Firma Digitale
- La Marca Temporale
- La Firma Elettronica Avanzata Grafometrica
- La Posta Elettronica Certificata
- Validità europea e regolamenti futuri

Le Firme Informatiche

Sono il nuovo modo per affermare l'identità dell'individuo che, anziché apporre la sua sottoscrizione su un documento reale, l'appone su uno informatico.

Il legislatore ha scelto un rapporto di equivalenza e non di identità tra le firme informatiche e la sottoscrizione autografa così come tra documento informatico e documento.

La firma non è necessariamente sottoscritta e non è più sempre e solo un gesto personalissimo dell'autore.

Normativa di riferimento

DLGS 07/03/2005, n. 82: CAD: Codice dell'Amministrazione Digitale

Entrato in vigore il 1° gennaio 2006.

… ha subito nel corso del tempo diverse modifiche , l'ultima delle quali nel dicembre del 2012 con il c.d. Decreto Crescita bis (d.l. 18 ottobre 2012, n. 179, convertito con Legge 17 dicembre 2012, n. 221)

La modifica più importante:

DPCM 22/02/2013: Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali

Pubblicate in Gazzetta Ufficiale il 21 maggio 2013, declinano nel dettaglio quanto è affermato nella normativa primaria.

Firme informatiche e il documento informatico

Bisogna abbandonare l'idea che un documento sia cartaceo e che una sottoscrizione sia autografa

DOCUMENTO INFORMATICO:

Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Il documento informatico reca in sé una nuova idea di documento e la firma informatica è diversa dalla sottoscrizione autografa.

Firma Elettronica (Semplice)

Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica

- Definizione di Firma tecnologicamente neutra: non si fa riferimento alla tecnologia utilizzata.
- Per esemplificare, si ritiene che in questa tipologia di firma rientrino nella definizione le firme basate:
  - su qualcosa che si è (c.d. firme biometriche, basate su caratteristiche fisiche/personali dell'individuo – impronte digitali, scansione della retina, riconoscimento vocale, ecc..)
  - su qualcosa che si ha, (un dispositivo, un oggetto – token, smart card, ecc..)
  - su qualcosa che si conosce (rientrano quelle tramite pin e password)
- Possono soddisfare requisiti di sicurezza elevati / «forti», quindi non è corretto definirle «firme Deboli».

Firma Elettronica Avanzata (FEA)

Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che:

- **consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario;**
- **creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati**

- Definizione Introdotta con una modifica normativa del CAD nel 2011, la piena operatività di questa firma è stata poi riconosciuta con la pubblicazione delle Regole Tecniche in GU.
- Definizione di Firma tecnologicamente neutra: non si fa riferimento alla tecnologia utilizzata, ma DEVE soddisfare determinati requisiti disciplinati nelle Regole Tecniche.
- E' essenziale comprendere che la FEA non si «riduce» al prodotto che viene utilizzato (tablet, OTP, ecc..), ma è qualificata come tale solo dal PROCESSO che viene adottato (Es. del medesimo tablet utilizzato sia in una Banca che da un corriere: le condizioni che precedono l'uso del Tablet sono diverse).

Firma Elettronica Qualificata (FEQ)

Particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma

- Si abbandona quindi la neutralità tecnologica e si fa riferimento a una tecnologia specifica che prevede l'uso di un certificato qualificato e l'utilizzo di un dispositivo sicuro per la creazione della firma.

Firma Digitale

Particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico

- Si tratta di una firma basata su una specifica tecnologia (c.d. a chiavi asimmetriche).

Efficacia probatoria del documento informatico senza firma

- **efficacia prevista dall'art. 2712* del codice civile (rinvio dall'art. 23 quater del CAD)**
- **efficacia probatoria delle riproduzioni meccaniche**
- **prova i fatti in esso rappresentati se non è disconosciuto**

Se viene prodotto in giudizio e non viene disconosciuto, costituisce piena prova dei fatti in esso rappresentati. Se viene validamente disconosciuto, non può più costituire piena prova dei fatti, ma degrada a elemento di prova che, insieme ad altri elementi di prova, potrà fondare il convincimento del giudice.

Efficacia probatoria del documento informatico con firma elettronica

- **efficacia probatoria e idoneità a soddisfare il requisito della forma scritta liberamente valutabili in giudizio**
- **riferimento a caratteristiche oggettive di sicurezza, integrità, qualità e immodificabilità**

Di volta in volta il giudice valuterà quanto siano «forti» quella determinata firma o quel determinato processo e giudicherà l'efficacia probatoria del documento a cui quella firma elettronica è associata.

I criteri a cui il giudice deve attenersi:

- Sicurezza e qualità del Sistema Informatico
- integrità e immodificabilità del documento Informatico.

Efficacia probatoria del documento informatico con firma elettronica avanzata, qualificata, digitale

- **Hanno tutti e tre le tipologie di documenti l'efficacia probatoria della scrittura privata (art. 2702* c.c.).**

Ci riferiamo alle tre tipologie di documenti informatici sottoscritti con FEA (firma grafometrica tramite tablet) o con firma qualificata o digitale (smart card e token basata sull'utilizzo di chiavi crittografiche).
Fanno piena prova della provenienza delle dichiarazioni da parte del firmatario.

IMPORTANTE DIFFERENZA

introdotta con il D.lsg 179 2012 tra doc. informatico con FEA e gli altri due.
Nel caso di doc. informatico sottoscritto con firma qualificata o digitale, l'utilizzo del dispositivo di firma si presume riconducibile al titolare salvo che questi ne dia prova contraria. Vige una presunzione di utilizzo del dispositivo di firma da parte del firmatario.
Tale presunzione NON vige nel caso di documenti informatici firmati con FEA (non c'è un dispositivo di firma: il cliente firma con la propria mano). Si applicano le norme sul disconoscimento previste dal codice di procedura civile.

***Art. 2702** *Efficacia della scrittura privata*

La scrittura privata fa piena prova, fino a querela di falso (Cod. Proc. Civ. 221 e seguenti), della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa e legalmente considerata come riconosciuta (Cod. Proc. Civ. 214, 215; Cod. Nav. 178, 775).

Schema sintesi

	Definizione	Valore probatorio	Esempi
Firma Elettronica	Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica	Efficacia probatoria valutabile dal giudice caso per caso	*Pin*, firma biometrica
Firma Elettronica Avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati	Efficacia probatoria della scrittura privata integra la forma scritta *ad substantiam* tranne che per i contratti immobiliari	Firma su *tablet*
Firma Elettronica Qualificata	Particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma	Efficacia probatoria della scrittura privata integra la forma scritta *ad substantiam*	*Smart-card*, *token*
Firma Elettronica Digitale	Particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici	Efficacia probatoria della scrittura privata integra la forma scritta *ad substantiam*	*Smart-card*, *token*

Il podio della sicurezza ma non dell'utilizzo

Firma Qualificata Firma Digitale

Firma Avanzata

Firma Semplice

- Premessa
- Le Firma informatiche
- **La Firma Digitale**
- La Marca Temporale
- La Firma Elettronica Avanzata Grafometrica
- La Posta Elettronica Certificata
- Validità europea e regolamenti futuri

Chi la rilascia e i requisiti del soggetto

La Firma Digitale viene rilasciata da un Ente Certificatore che:

- Rilascia, gestisce, pubblica e revoca i certificati;
- Certifica la chiave pubblica di un soggetto;
- Rende certa l'identità del soggetto fisico che ha generato una firma, assicurando la corrispondenza tra il titolare e la sua chiave pubblica.

I requisiti necessari per avere una firma digitate:

- Essere in possesso di Codice Fiscale;
- Essere in possesso di un documento d'identità valido;
- Aver compiuto 18 anni;
- Disporre di una casella mail non certificata per tutte le comunicazioni da parte del Certificatore, anche le credenziali di accesso
- Essere residente o con domicilio fiscale in Italia

I componenti del sistema

Certificati di firma qualificati su dispositivo o remoto:

- *Smart Card (eventualmente con lettore)*

- *Token USB*

- *MicroSD*

- *Firma remota su dispositivi HSM (OTP, SMS PIN, etc..)*

Software per l'apposizione di firme digitali.

PC, Tablet, Smartphone

Il certificato digitale di sottoscrizione

L'elemento di rilievo è il **certificato digitale di sottoscrizione** che l'Ente Certificatore rilascia al titolare del dispositivo di firma.

Il certificato è un **file generato seguendo precisi standard** stabiliti per legge, contiene informazioni sull'identità del titolare, sulla chiave pubblica che gli è stata attribuita al momento del rilascio, sul periodo di validità del certificato stesso. Nel certificato sono presenti anche le info sull'Ente Certificatore.

Il certificato digitale di un titolare, una volta entrato a far parte dell'elenco pubblico dei certificati tenuto dall'ente Certificatore, garantisce la **corrispondenza tra la chiave pubblica e l'identità del titolare**.

La validità del certificato digitale

Il certificato digitale è un documento di identità nel mondo digitale.

Un Certificato ha un periodo di validità (mediamente 3 anni) ma prima della scadenza può essere SOSPESO o REVOCATO.

La Revoca o Sospensione viene segnalata pubblicando liste di revoca e sospensione (CRL).

Una Firma Digitale non è valida se non lo è il suo Certificato.

Funzioni del processo di firma digitale

- **Identificazione**

Indica con certezza chi è il mittente di un messaggio o documento elettronico. In molte occasioni è indispensabile che le due parti in comunicazione **conoscano la controparte remota**.
L'identificazione elettronica rende possibile identificare un utente, un cliente, un partner grazie a strumenti elettronici.

- **Firma**

Garantisce che il documento non è stato modificato dopo la sua sottoscrizione e gli dà uno status legale. E' importante che le informazioni **siano originali**, **non modificate** durante la trasmissione, accidentalmente o intenzionalmente.
La firma elettronica permette al mittente di firmare il messaggio cosicché il destinatario possa sapere con certezza chi l'ha spedito e che l'informazione non è stata alterata. Ciò tra l'altro impedisce che il mittente possa in seguito disconoscere la paternità del documento (non ripudiabilità)

Formati di firma

CAdES

(CMS Advanced Electronic Signature)

Qualsiasi file .doc, .xls, .exe, .pdf, .ppt etc….

L’estensione del file firmato è **.p7m**

PAdES

(PDF Advanced Electronic Signature)

Solo file .pdf

L’estensione del file firmato è .pdf

XAdES

(XML Advanced Electronic Signature)

Solo file .xml

L’estensione del file firmato è .xml

Caratteristiche del documento firmato digitalmente

Integrità
Garanzia che il documento informatico non è stato manomesso dopo la sua sottoscrizione;

Non ripudio
La firma digitale si presume riconducibile al titolare del dispositivo di firma, salvo che sia data prova contraria

Autenticità
certezza dell'identità del sottoscrittore;

Valore legale
il documento informatico sottoscritto con firma digitale soddisfa il requisito legale della forma scritta se formato nel rispetto delle regole tecniche stabilite dalla legge che garantiscono l'identificabilità dell'autore e l'integrità del documento.

- Premessa
- Le Firma informatiche
- La Firma Digitale
- **La Marca Temporale**
- La Firma Elettronica Avanzata Grafometrica
- La Posta Elettronica Certificata
- Validità europea e regolamenti futuri

La marcatura temporale

Un altro dei fattori che fanno sicura e affidabile la firma digitale è la **marcatura temporale (time stamping)**. Questa garantisce data e ora certi per un documento informatico al momento dell'apposizione.

Il servizio di marcatura temporale di un documento informatico, consiste nella generazione, da parte di una Terza Parte Fidata, di una firma digitale del documento (anche aggiuntiva rispetto a quella del sottoscrittore) cui **è associata l'informazione relativa ad una data e ad un'ora certa**.

Un file marcato temporalmente (con estensione .m7m) al suo interno contiene il documento del quale si è chiesta la validazione temporale la marca emessa dall' Ente Certificatore.

Caratteristiche fondamentali:

- mantiene la validità del documento oltre la validità del certificato;
- prova l'esistenza di un documento ad un determinato istante.

Perché è importante?

Nell'ambiente digitale è importante assegnare una data e un'ora certa ad un documento per mostrare quando è stato scritto e firmato (ad esempio gare e concorsi).

La marca temporale convalida il documento, anche certificando che l'ID del suo firmatario era valido al momento della firma. L'uso della marca temporale non tocca il contenuto del documento e non ne modifica la sua firma.

Il tempo, cui fanno riferimento le marche temporali, è riferito al Tempo Universale Coordinato ed è assicurato da un ricevitore radio sintonizzato con il segnale emesso dall'istituto nazionale di Ricerca Metrologica.

Un documento firmato digitalmente e marcato temporalmente ha valenza legale superiore al corrispondente cartaceo con firma autografa.

Se il documento viene anche trasmesso via PEC il procedimento ha una valenza legale ancora più forte.

Un documento firmato digitalmente e marcato temporalmente ha valenza legale superiore al corrispondente cartaceo con firma autografa.

Se il documento viene anche trasmesso via PEC il procedimento ha una valenza legale ancora più forte.

- Premessa
- Le Firma informatiche
- La Firma Digitale
- La Marca Temporale
- **La Firma Elettronica Avanzata Grafometrica**
- La Posta Elettronica Certificata
- Validità europea e regolamenti futuri

Perché la Firma Qualificata stenta a partire?

Le motivazioni per cui la **Firma Qualificata** (rilasciata su dispositivi sicuri quali smartcard, token o firma remota con autenticazione forte OTP) **non ha avuto una diffusione e il successo che ci si aspettava** è da individuarsi in diversi fattori:

- Necessità di **"avere con sé" un dispositivo** e ricordarsi (nel caso di firma locale) un codice numerico
- Complicata **usabilità del software** di firma (non sempre è di semplice utilizzo)
- **Complessità di installazione** dei dispositivi (sistemi operativi, antivirus etc…)
- **Modesta diffusione** del sistemi di lettura (lettori di smartcard in particolare)
- I documenti firmati digitalmente **non riportano** (tranne per i pochi che inseriscono il logo in pdf) **evidenza visuale** (grafica) dell'essere stati firmati (fortissima barriera psicologica)
- **Rilascio complesso** e poco presente sul territorio
- Allargamento del **digital divide**
- **Scarsa culturizzazione** sull'argomento per il personale a contatto con il pubblico per cui quasi inesistente invito all'utilizzo (diffusione prevalente nelle ragioni sociali attraverso i commercialisti)
- **Pochi servizi** con possibilità di utilizzo
- **Scarsa comunicazione** mirata
- **Innata diffidenza** e resistenza alle novità (10 anni per accettare il bancomat)
- **Vantaggi** per il cittadino, se esistenti, **non evidenti**
- Processo di **difficile divulgazione** e ancor più difficile comprensione (solo per addetti ai lavori)

Interpretazioni sulla Firma Grafometrica

RICONOSCIMENTO

I dati grafometrici possono essere utilizzati come strumento di riconoscimento di un soggetto che abbia in precedenza provveduto a depositare alcuni "specimen" del proprio comportamento durante la sottoscrizione.

Il successivo confronto tra i dati conservati e quelli rilevati al momento permettono di riconoscere - con un margine di errore - il soggetto sottoscrittore, e di autenticarlo presso un certificatore di firma digitale permettendo, così, l'apposizione di una sua firma digitale limitata al contesto sul documento da sottoscrivere.

SOTTOSCRIZIONE

I dati grafometrici possono essere utilizzati in differenti processi che permettono di sottoscrivere i documenti con una firma elettronica "semplice" o, ad alcune condizioni, una Firma Elettronica Avanzata (FEA).

I dati grafometrici non vengono conservati in separati archivi per i successivi confronti, ma vengono criptati e "fusi" con il documento stesso. Solo nel caso di disconoscimento della firma, si provvederà a decifrare i dati grafometrici contenuti nel documento e a confrontarli con quelli presenti in altri documenti già verificati o con quelli raccolti al momento stesso dal perito grafologo nominato dal giudice.

Soluzione Namirial

Cos'è FirmaGrafoCerta

La soluzione di Firma Grafometrica di Namirial S.p.A. è un **processo di Firma Elettronica Avanzata** Autografa che ha come prerogativa la presenza di una Autorità di Certificazione (CA) e la presenza di un operatore di front-end (operatore di sportello, addetto ufficio etc…) che presiede all'atto della firma dell'utente e ne convalida la sua presenza.

Così pensato e realizzato soddisfa i requisiti di identificabilità dell'autore della firma generata, così come l'integrità e l'immodificabilità del documento informatico.

Riduzione del rischio di illeciti

Il rischio di illeciti non aumenta rispetto ad un flusso cartaceo perché viene riproposto; anzi, in termini assoluti, il **rischio viene ridotto**.

Se un cliente disconosce la firma sul cartaceo lo può fare anche con il processo FirmaGrafoCerta con la differenza che, deve provare sia che non era ne davanti alla persona che lo ha riconosciuto firmando digitalmente, sia che (in caso di marca temporale) non era davanti all'operatore in quel determinato momento.

Se è valido ed accettato dai legali il flusso cartaceo,
lo è anche il processo FirmaGrafoCerta

Art. 58 - Certificazione ISO 27001:2005

Come previsto dalle regole tecniche nel DPCM del 22 febbraio 2013 chi fornisce una soluzione di firma elettronica avanzata alle pubbliche amministrazioni, **deve essere in possesso della certificazione di conformità** del proprio sistema di gestione per la sicurezza delle informazioni, alla norma **ISO/IEC 27001, rilasciata da un terzo indipendente a tal fine autorizzato secondo le norme vigenti in materia.**

BUREAU VERITAS
Certification

Certification

Awarded to

NAMIRIAL SPA

LEGAL AND OPERATIVE SITE:
V. Caduti sul lavoro 4
60019 Senigallia (AN) - ITALY

Bureau Veritas Italia certify that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27001:2005

Scope of supply

PRODUCTION OF ADVANCED DIGITAL SIGNATURE SOLUTIONS, AIMING TO PUBLIC ADMINISTRATION AND PRIVATE ORGANIZATION THROUGH USING BIOMETRIC SOFTWARE DATA CAPTURE AND CODING SYSTEM ACCORDING TO THE CURRENT REGULATIONS.

STATEMENT OF APPLICABILITY REV. 01 AS OF JANUARY 13, 2012

Namirial ha ottenuto la certificazione ISO27001:2005 sul processo di firma grafometrica rilasciata da un Ente accreditato.

Elementi del sistema: software e certificati

- Software ***Namirial FirmaCerta***
- App FirmaGrafoCerta

<u>con abilitazione per la funzionalità di firmagrafometrica</u>

Certificati di protezione dei dati biometrici

- Componente pubblica che cifra distribuita sui terminali;
- Componente privata che decifra conservata secondo procedura;

Certificati di marcatura temporale (opzionale)

Connessione internet per l'apposizione della marca

Certificati di firma qualificati su dispositivo o remoto (Strong):

- *Smart Card*

- *Token USB*

- *MicroSD*

- *Firma remota su dispositivi HSM*

Certificati di firma privati su terminali (Medium):

- *File*

Elementi del sistema: hardware

Soluzioni per postazioni fisse

Soluzioni (plug&play) – Da connettere ad un terminale con Windows XP e superiori, ideale per postazioni di sportello.

Soluzioni per postazioni mobili

Nuovi dispositivi con Windows 7, Windows 8 e Android che si differenziano per le caratteristiche tecniche e per le periferiche; in comune hanno tutti **lo schermo con rilevazione dell'indice pressorio**, elemento obbligatorio per gestire la firma grafometrica.

Innesto con la conservatoria digitale

Una volta che i documenti vengono sottoscritti, devono essere conservati in luogo sicuro in quanto non esiste più la «sicurezza percepita» dello stoccaggio del cartaceo.

Non si parla più di sostitutiva ma di **conservatoria digitale a norma di legge**.

Un documento firmato grafometricamente trova la sua naturale archiviazione su strumenti informativi che gestiscono la conservazione a norma di legge.

Declinazioni Soluzione GrafoCerta

Il processo FirmaGrafoCerta può essere **adattato al tipo di documento** che si sta sottoscrivendo e al livello di rischio che l'Ente erogante il servizio si vuole assumere.

Tale rischio può non essere sempre uguale per tutti i documenti e, nello stesso documento, per tutte le firme.

Su richiesta di clienti sono state quindi declinate 3 diverse soluzioni:

- **FORTE (Strong)** – certificato di protezione dei dati biometrici – certificato di firma qualificato su dispositivo per ogni operatore
- **MEDIA (Medium)** – certificato di protezione dei dati biometrici – certificato di firma privato su file (personale o uguale per tutti gli operatori)
- **LEGGERA (Light)** – acquisizione del solo tratto grafico;

Il contenzioso grafologico

In caso di contenzioso si andrà di fronte al giudice analogamente al cartaceo. Questo presuppone che il grafologo sia in grado di analizzare e interpretare i dati biometrici.

Partendo dal presupposto che la perizia grafica su base grafologica non ha come scopo l'analisi di personalità ma **l'analisi identificatoria della scrittura**, cioè definire e distinguere la produzione grafica di un individuo da quella di qualsiasi altro individuo è nata la collaborazione tra la Grafologia (AGI) e l'Informatica (Namirial) con l'obiettivo di aiutare i tecnici peritali ad avere strumenti atti ad esercitare la professione con le nuove tecnologie.

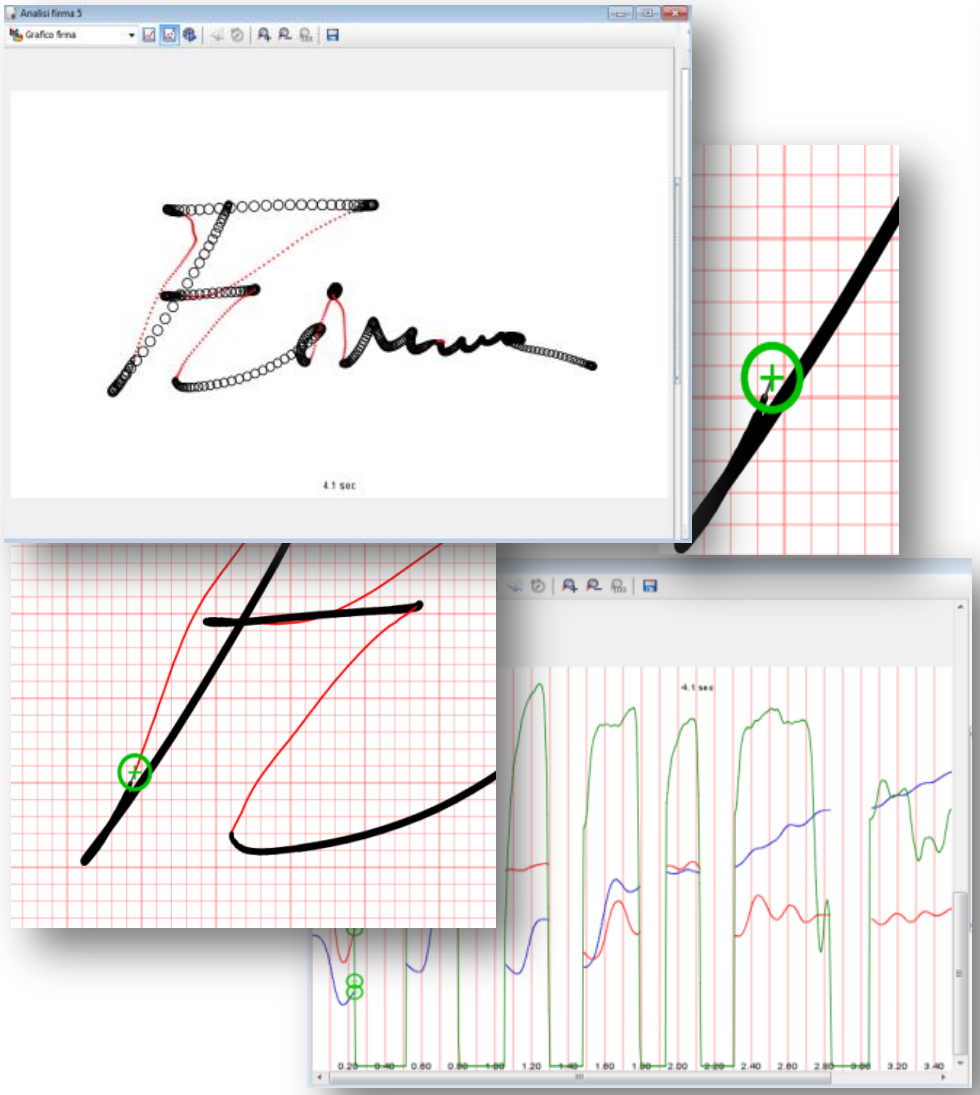
- Analisi firme grafometriche
- Interpretazione dei dati biometrici

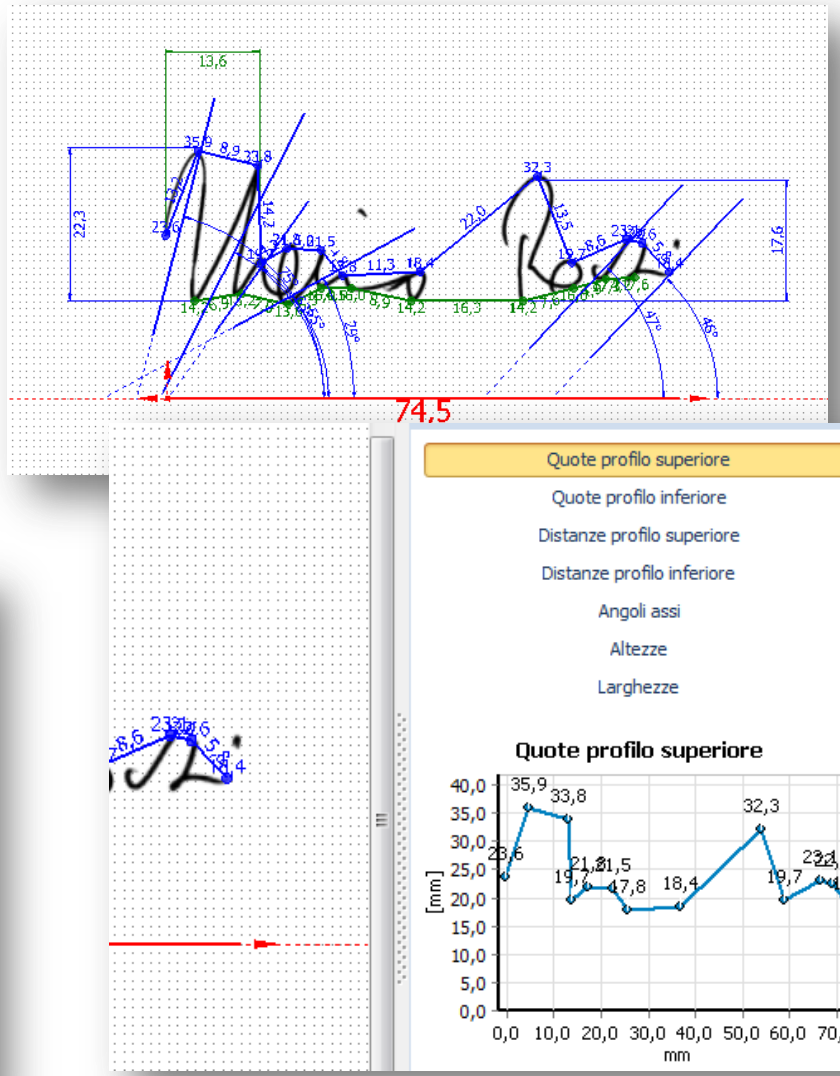
FirmaCerta Forense

- Analisi delle immagini con rilevamento misure
- Redazione della perizia

Namirial Grafologico

Esempi di risultati





- Premessa
- Le Firma informatiche
- La Firma Digitale
- La Marca Temporale
- La Firma Elettronica Avanzata Grafometrica
- **La Posta Elettronica Certificata**
- Validità europea e regolamenti futuri

PEC – Posta Elettronica Certificata (1/2)

Il decreto legge **185** del **29 novembre 2008** ha stabilito l'obbligo, per le *società di capitali*, *per le società di persone* e per i *professionisti* iscritti in albi o elenchi e *le pubbliche amministrazioni*, di dotarsi di una casella di posta elettronica certificata (PEC):

- per i **professionisti** (avvocati, ingegneri, architetti, consulenti del lavoro, dottori commercialisti ed esperti contabili, farmacisti, dottori, infermieri etc....) è diventata obbligatoria dal **29/11/2009** e doveva essere comunicata all'ordine o collegio di appartenenza;

- per le **amministrazioni pubbliche** che non vi avessero ancora provveduto ai sensi dell'art. 47, comma 3, lettera a), del Codice dell'Amministrazione digitale (CAD) devono istituire una casella di posta certificata per ciascun registro di protocollo e ne danno comunicazione ad AGiD (ex DigitPA - ex CNIPA).

PEC – Posta Elettronica Certificata (2/2)

- per le **società di nuova costituzione** la PEC è obbligatoria e deve essere richiesta alla costituzione della società (la mancata comunicazione dell'indirizzo PEC determina la sospensione del procedimento di iscrizione al Registro Imprese);

- per le **società già costituite al 29/11/2008** la PEC doveva essere richiesta entro e non oltre il 29/11/2011 e doveva essere comunicata al Registro Imprese competente;

Dal 21 ottobre 2012 anche le **imprese individuali** che si iscrivono al registro delle imprese o all'albo delle imprese artigiane **devono dotarsi di una casella di posta elettronica certificata (PEC)**.
Quelle già costituite hanno tempo fino al 30 giugno 2013.

Ma lo Stato non ha fornito una PEC gratuita a tutti i cittadini? Cosè la CEC-PAC?

PEC- Definizioni

Che cos'è la PEC?

La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica (che utilizza i protocolli standard della posta elettronica tradizionale) nel quale al mittente viene fornita, in formato elettronico, la prova legale dell'invio e della consegna di documenti informatici.

A cosa serve?

Alla trasmissione di messaggi, che possono contenere qualsiasi tipologia di informazione ed allegato, di cui si vuole avere la certezza della consegna. La PEC è nata per sostituire, attraverso i moderni mezzi di comunicazione, la Raccomandata postale con ricevuta di ritorno, o raccomandata AR.

Così come avviene per la raccomandata AR, al mittente viene inviata una ricevuta che attesta la consegna al destinatario del proprio messaggio.

Garanzia sulla trasmissione, ricezione e sicurezza dei messaggi

PEC – Il flusso operativo

Ricevute di ACCETTAZIONE e CONSEGNA

"Certificare" l'invio e la ricezione (i due momenti fondamentali nella trasmissione dei documenti informatici) significa che il gestore di posta del mittente fornisce una ricevuta che costituisce prova legale **dell'avvenuta spedizione** del messaggio e dell'eventuale allegata documentazione.

Allo stesso modo, quando il messaggio perviene al destinatario, il gestore invia al mittente la ricevuta di **avvenuta (o mancata) consegna** con precisa indicazione temporale.

Dal punto di vista dell'utente, una casella di posta elettronica certificata non si differenzia dunque da una casella di posta normale; cambia solo per quello che riguarda il meccanismo di comunicazione sul quale si basa la PEC e sulla presenza di alcune ricevute inviate dai gestori PEC al mittente e al destinatario.

Il flusso funziona correttamente ed ha piena validità legale da PEC a PEC.

E come funziona da PEC a non PEC?
E da non PEC a PEC?

PEC – Il flusso operativo

PEC – L'utilizzo e il rilascio

Per poter utilizzare la PEC si deve disporre di un'apposita casella di PEC, fornita da gestori autorizzati (comunicazione con qualsiasi tipo di casella postale elettronica e completa funzionalità) attraverso una precisa procedura di riconoscimento.

La pubblicazione dell'elenco dei gestori autorizzati e quello della Pubblica Amministrazione, la vigilanza e il coordinamento nei confronti dei gestori e della Pubblica Amministrazione è demandata all'Ente nazionale per la digitalizzazione della Pubblica Amministrazione (AGID ex DigitPA).

Il Governo italiano fornisce gratuitamente una casella di PEC che in realtà si chiama CEC-PAC (Comunicazione Elettronica Certificata – Pubblica Amministrazione Cittadino) che è limitata alle sole comunicazioni con la Pubblica Amministrazione su un dominio specifico e senza firma digitale). Se si vuole estendere bisogna pagare alle Poste come si farebbe con altri gestori.

Chi attiva la CEC-PAC è meglio che la controlla costantemente

PEC – Le caratteristiche (1/2)

Semplicità: il servizio PEC si usa come la normale posta elettronica sia tramite programma cliente (es. Outlook Express), sia tramite web mail, sia tramite programmi ad hoc. Si può leggere da qualsiasi dispositivo computer o smartphone.

Sicurezza: il servizio utilizza i protocolli sicuri POP3s, IMAPs, SMTPs ed HTTPs. Tutte le comunicazioni sono protette perché crittografate e firmate digitalmente. Per questo avrete sempre la certezza che i messaggi inviati o ricevuti non possano essere contraffatti

Valore legale: a differenza della tradizionale posta elettronica, alla PEC è riconosciuto pieno valore legale e le ricevute possono essere usate come prove dell'invio, della ricezione ed anche del contenuto del messaggio inviato.

No virus e spam: l'identificazione certa del mittente di ogni messaggio ricevuto ed il fatto che non si possano ricevere messaggi non certificati, rendono il servizio PEC pressoché immune dallo spam.

PEC – Le caratteristiche (2/2)

Costo fisso: il prezzo annuale di una casella PEC non prevede costi aggiuntivi in base all'utilizzo. Cambia sulla base dei servizi opzionali che si attivano (dimensione casella, conservazione etc…).

Garanzia di qualità e continuità del servizio: I Service Level Agreement (SLA) di legge prevedono una disponibilità del servizio del 99,8% su base quadrimestrale. Gli SLA della disponibilità del servizio PEC non valgono per la connettività. In altri termini, i server del gestore PEC possono essere disponibili nel 99,8% dell'anno, ma la connettività per raggiungerli (offerta da una terza parte) potrebbe avere SLA differenti.

Conservazione: c'è l'obbligo da parte del gestore di archiviare tutti gli eventi associati a invii e ricezioni (log) di messaggi PEC, per un periodo di trenta mesi.

Privacy: c'è l'obbligo da parte del gestore di applicare le procedure atte a garantire il rispetto delle misure di sicurezza previste dal Codice dei dati personali e la sicurezza della comunicazione.

PEC – Confronto con altri mezzi

Nello schema di seguito un confronto tra la PEC e gli strumenti tradizionali di trasmissione

Voci	Posta prioritaria	Raccomandata semplice	Raccomandata AR	Fax	Corriere Espresso	Casella mail semplice	Casella PEC
invio da casa/ufficio	**NO**	**NO**	**NO**	**SI**	**SI**	**SI**	**SI**
Valore legale	**NO**	**SI**	**SI**	**SI**	**NO**	**NO**	**SI**
Consegna Immediata	**NO**	**NO**	**NO**	**SI**	**NO**	**SI**	**SI**
Certificazione Avvenuta spedizione	**NO**	**SI**	**SI**	**SI**	**SI**	**NO**	**SI**
Avviso di ricezione	**NO**	**NO**	**SI**	**SI**	**SI**	**NO**	**SI**
Mantenimento ricevuta	**NO**	**SI**	**SI**	**NO**	**SI**	**NO**	**SI**
Inalterabilità del contenuto	**SI**	**SI**	**SI**	**SI**	**SI**	**NO**	**SI**
Costo unitario	a partire da 0,6	a partire da 2,8	a partire da 3,6	in funzione dell'operatore	in funzione del corriere	**NO**	SI
Costo fisso	-	-	-	-	-	-	SI
Risparmio su costi aggiuntivi	**NO**	**NO**	**NO**	**NO**	**NO**	**SI**	**SI**

PEC – Dati attivazioni (fonte AgID)

Nello schema di seguito i dati di attivazioni dei domini delle caselle e dei messaggi inviati.
Dal 2009 al 2013 (non ancora terminato):
- Il numero di caselle è 7 volte di più
- Il numero di messaggi e il numero di domini sono triplicati

ANNO	BIMESTRE	DOMINI	CASELLE	MESSAGGI
2009	6	70.641	1.354.003	43.148.977
2010	6	110.213	2.208.174	52.822.623
2011	6	180.727	4.395.580	57.956.664
2012	6	202.694	4.918.637	91.488.442
2013	5	226.357	7.733.110	128.773.178

Conservazione delle PEC

Il provider PEC ha l'obbligo di conservazione dei Log delle ricevute per 30 mesi.

E se si vuole una conservazione sicura anche delle ricevute e delle PEC? E per un periodo più lungo?

- SOLUZIONI OPZIONALI:
- Accordo con il provider PEC per allungare i tempi di conservazione dei log oltre i 30 mesi (es: avvocati con il Processo Civile Telematico);
- Accordo con il provider PEC per conservare anche le ricevute e non solo i log;
- Accordo con il provider PEC per conservare a norma di legge sia le PEC inviate con le loro ricevute di accettazione e consegna, sia la PEC in arrivo.
- Dotarsi di applicativi disegnati ad hoc per la gestione e l'eventuale conservazione dei file;

E se una PEC deve essere gestita da più persone (previa sottoscrizione di delega all'uso)?

- Per poter gestire sia le PEC inviate che quelle in arrivo devono essere adottati strumenti ad hoc per la gestione multipla di singole caselle PEC (vedi PECMailer Pro)

PEC - i limiti nella sua gestione attuale (1/2)

Invio mail e gestione delle ricevute

Per inviare e ricevere le mail è possibile utilizzare la WebMail o qualsiasi altro client di posta elettronica.

Una mail spedita a 50 destinatari comporta al massimo la ricezione di 100 ricevute tra accettazione, consegna ed anomalia. La mail inviata andrà nella cartella posta inviata mentre le ricevute nella cartella posta ricevuta andando a confondersi con tutto il resto della corrispondenza.

Diventa fondamentale capire se le ricevute di accettazione e consegna sono arrivate e avere un collegamento tra l'email inviata e le ricevute stesse.

Gestione dello spazio

Nel caso di invio massivo, se i destinatari sono 1.000 si ricevono 2.000 ricevute tra accettazione, consegna e anomalia. Le ricevute, sebbene a scelta dell'utente e/o del provider, sono di dimensioni confrontabili con la mail di partenza. Siamo sicuri di non intasare il server e destabilizzare il provider?

E' importante monitorare sempre lo spazio e non rischiare di creare danni involontari sulla rete.

PEC - i limiti nella sua gestione attuale (2/2)

Invio della PEC in CCn per il rispetto della privacy.

La PEC non può essere inviata a destinatari in CCn (Copia Conoscenza Nascosta) perché per sua natura è necessaria la certezza di chi l'invia e a chi è consegnata .

Questo significa che un invio a più destinatari contemporaneamente fatto con un mailer standard metterebbe in evidenza tutti gli indirizzi.

Diventa necessario uno strumento che a partire da un'unica mail da inviare ad un gruppo di destinatari crei per ognuno una singola comunicazione.

Verifica dell'esito dell'invio

L'invio della PEC inviata a multidestinatari deve essere di immediata verifica. Con i mailer standard non è possibile avere la sintesi dell'esito dell'invio ma la ricerca va fatta manualmente per singola ricevuta.

Archiviazione PEC e ricevute

I gestori hanno l'obbligo di mantenere dei soli log degli invii PEC per 30 mesi. Se per un motivo incidentale vengono perse le PEC e le ricevute nessuno le può restituire.

E' indispensabile prevedere un'archiviazione sicura della comunicazione indipendentemente dai log.

PEC – Come avviare ai limiti esposti?

Sono disponibili sul mercato diversi software.

La soluzione Namirial **– chiamata PECMailer -** è un semplice ma completo *client* di posta elettronica che consente di gestire la composizione, la trasmissione, la ricezione e l'organizzazione di messaggi di ***Posta Elettronica Certificata (PEC)*** da e verso un server di posta. Il *client* si occupa della composizione e della lettura, mentre il *server* (il gestore del servizio) si occupa della trasmissione dei messaggi.

La peculiarità di PECMailer consiste nella capacità di riconoscere le ricevute di *Consegna* da quelle di *Accettazione* (o di Anomalia) e conservarle in una cartella ad esse dedicata.

L'applicativo consente in maniera semplice e veloce di gestire le comunicazioni massive attraverso PEC. Di semplice utilizzo, affianca e non sostituisce o interferisce con il client di posta elettronica preconfigurato sul PC come Outlook ,Windows Mail etc.
Il software è stato realizzato per la gestione di ***account PEC*** con gestione singola (versione client) sia con gestione multipla (versione client-server).

- Premessa
- Le Firma informatiche
- La Firma Digitale
- La Marca Temporale
- La Firma Elettronica Avanzata Grafometrica
- La Posta Elettronica Certificata
- **Validità europea e regolamenti futuri**

Situazione attuale

Nel caso di firme digitali basate su certificati emessi da Autorità di Certificazione autorizzate nei diversi Stati membri dell'Unione Europea c'è la possibilità di riconoscere documenti informatici sottoscritti con firma digitale emessa.
Alcune firme apposte con modalità di criptazione datate sono valide in alcuni Paesi e non in altri.

Nel caso di partecipazioni a bandi di gara con invio della documentazione in formato elettronico, la firma digitale è un'alternativa ma deve essere del Paese che ha indetto il bando. Quindi un canadese che vuole partecipare ad una gara italiana deve acquistare una firma digitale italiana.

Cenni al nuovo regolamento europeo

E’ in fase di stesura il regolamento europeo sulle firme elettroniche.
Un regolamento non si recepisce, si applica quando entra in vigore.
Il regolamento definisce:

- le regole per l’identificazione elettronica e i servizi elettronici certificati;
- le regole secondo le quali uno Stato membro riconosce e accetta l’identificazione elettronica emessa da un altro Stato membro;

Con servizi certificati si intendono tutti i servizi elettronici volti alla creazione, alla verifica, alla validazione e alla salvaguardia delle firme elettroniche, marcature elettroniche, sistemi di delivery dei documenti, autenticazioni web e certificati elettronici.

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market.

Dettagli regolamento

E’ composto da 42 articoli, molto innovativo e complesso. Contiene eID (identificazione elettronica), firme, posta raccomandata (REM), conservazione e tanto altro.

Molto discusso tra i governi UE e nella concitata fase degli emendamenti. L’Italia è molto attiva.

Dovrebbe essere operativo a fine 2014 e l’Italia dovrà essere attenta a mantenere solide nel Regolamento alcune peculiarità del suo attuale ordinamento (PEC, firme, schemi di identificazione federata).

Introduzione della REM (Registered Electronic mail) al posto della PEC. All’85% sarà la stessa cosa, per gli utenti il passaggio sarà trasparente quindi la PEC attuale sarà adeguata ma sempre valida.

www.sicurezzadigitale.net

Email: luigi.tomasini@namirial.com

PEC: luigi.tomasini@sicurezzapostale.it