Namirial®
INFORMATION TECHNOLOGY
OUTSOURCING - STAFF TRAINING

La sicurezza nei dispositivi e token per scambio dati cifrati

Trento, 07 maggio 2012

L'autenticazione avanzata di Namirial: dal token e certificato pubblico alla firma con tavoletta biometrica

Ing. Luigi-Enrico Tomasini

SINCERT
Certificazione N. 223776

Namirial®
INFORMATION TECHNOLOGY
OUTSOURCING - STAFF TRAINING

CONTENUTI

- INTRODUZIONE: L' AZIENDA
- LA DEMATERIALIZZAZIONE
- LA FIRMA ELETTRONICA AVANZATA
- LA SOLUZIONE NAMIRIAL
- CONCLUSIONI

CHI SIAMO

Namirial S.p.A. è una Innovation company, a capitale interamente italiano, che ha trovato una propria specifica collocazione all'interno dei settori quali Information Technology, Business Process Outsourcing, Staff training, fornendo la propria offerta di servizi sull'intero territorio nazionale con strutture di proprietà.

Namirial eroga prodotti e servizi nei settori vitali dell'economia italiana come **strutture private** (Aziende, Professionisti, Istituti bancari) e **strutture pubbliche** (Enti, Ordini, Associazioni) che hanno necessità di operare sul territorio nazionale ed internazionale (anche in modalità molto distribuita) con propri punti operativi (sedi, filiali, basi, ecc.) governati e governabili da strutture gerarchicamente definite e pianificate.

La società ha la sede principale a Senigallia in una moderna struttura dove sono impiegati un centinaio di specialisti con una grande prevalenza di laureati in discipline scientifiche e tecnologiche (informatica, fisica, matematica, ecc.).
All'interno della azienda è operativo un'**Internet Data Center** dotato di tutti i sistemi di sicurezza necessari alla sicurezza della struttura ed in grado di supportare gli utenti anche per quanto concerne eventuali necessità di hosting, housing e colocation server.

I NUMERI NAMIRIAL

- Produzione 2010: 15,71 Mio€
- 125 Dipendenti;
- Nel 2011 oltre 2.000.000 di dichiarazioni dei redditi elaborate con i nostri software e transitate sui nostri server;
- Oltre 250.000 PEC emesse;
- Oltre 40.000 cedolini mensili elaborati;
- Oltre 50.000 clienti soddisfatti;

CERTIFICAZIONI E SEDI

- Ente Certificatore accreditato 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.

- Certificazione UNI EN ISO 9001:2008. Namirial ha conseguito il certificato n. 223776 rilasciata da Bureau Veritas Italia S.p.A.

Direzione generale: Senigallia (AN)

Sedi: Ancona (AN)
Avellino (AV)
Belgioioso (PV)
Gallarate (VA)
Modica (RG)

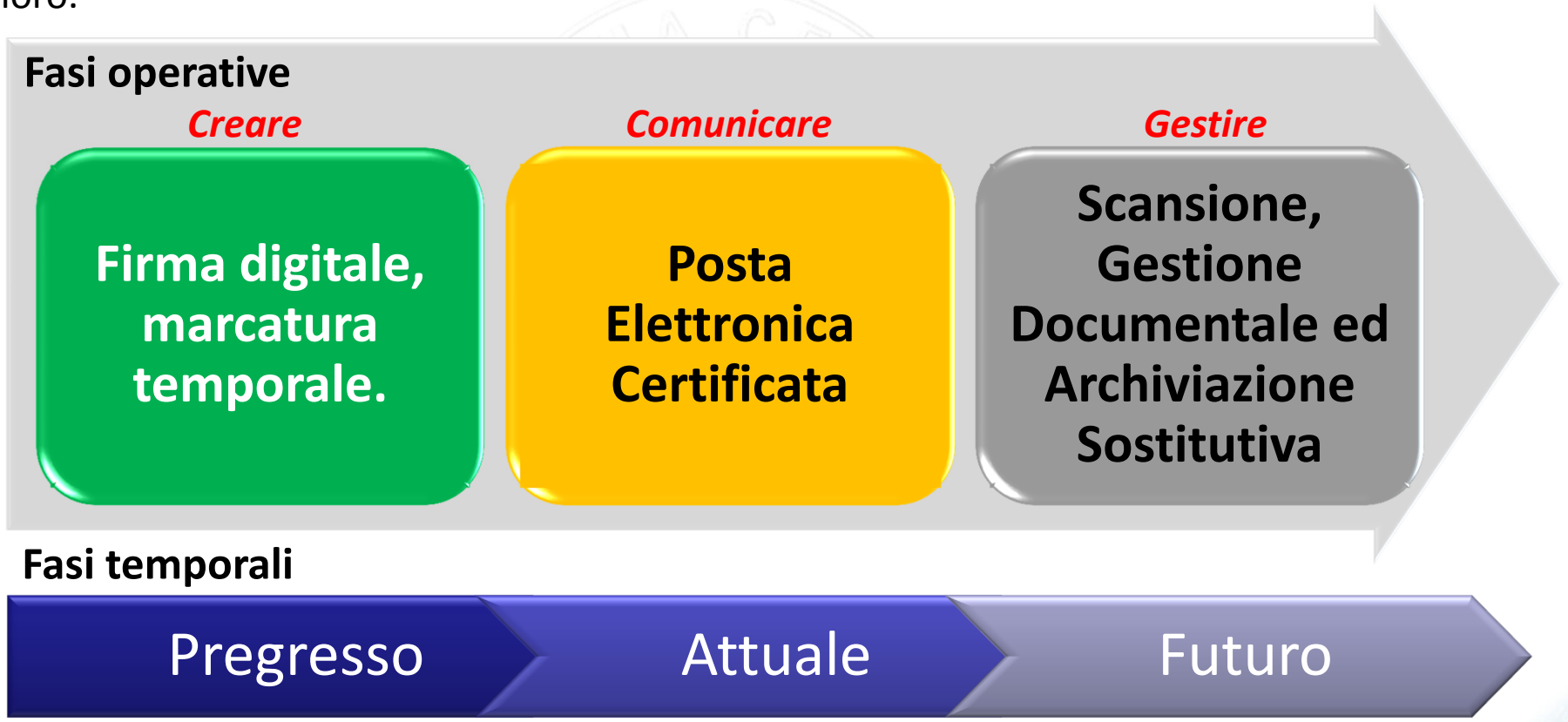
Certificazione N. 223776

CONTENUTI

- INTRODUZIONE: L' AZIENDA
- LA DEMATERIALIZZAZIONE
- LA FIRMA ELETTRONICA AVANZATA
- LA SOLUZIONE NAMIRIAL
- CONCLUSIONI

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.



Il CAD: passo avanti verso la dematerializzazione

22 dicembre 2010: **approvato** dal Consiglio dei Ministri, in via definitiva, lo schema del **nuovo Codice dell'Amministrazione Digitale (CAD)**, che fa seguito al Codice (dgls 82/05) varato nel 2005 e completa la riforma della Pubblica Amministrazione stabilita con il Dl 150/2010.

Il CAD non disciplina l'uso del digitale solamente nella Pubblica Amministrazione, ma definisce anche il *documento elettronico*, stabilisce *le regole dell'archiviazione sostitutiva*, regolamenta *l'uso della firma digitale* e della *Posta Elettronica certificata* (PEC).

Il **5 agosto 2011** è stata pubblicata la bozza delle regole tecniche in materia di documento informatico, gestione documentale e sistema di conservazione dei documenti informatici.

L'ADOZIONE DELLA DEMATERIALIZZAZIONE TROVA DEI BLOCCHI.....

Principali ostacoli al cambiamento

Normativi

- Dubbi da parte della direzione dell'Ente/Azienda che affronta l'argomento per la **validità legale** delle soluzioni e/o sulla complessità per dare un'effettiva validità legale (vedi processi di conservazione sostitutiva)

Organizzativi

- Difficoltà nel gestire il cambiamento da parte di chi decide di implementarlo e quindi da parte degli operatori; **impatti su processi, organizzazione, risorse umane**

Culturali

- Difficoltà culturale da parte di chi "subisce" il cambiamento, quindi degli utenti finali; **Digital Divide** è il divario che esiste nell'accesso reale alle nuove tecnologie

….CHE POSSONO ESSERE SUPERATI

Superamento di dubbi e ostacoli

Normativi

- Il nuovo CAD ha già fatto chiarezza su molti aspetti legati alla dematerializzazione ed è prevista a brevissimo la delibera sulle **regole tecniche** che daranno piena **validità** alle copie cartacee e digitali dei documenti informatici

Organizzativi

- I cambiamenti organizzativi sono gestibili con progetti specifici interni alle aziende, che prevedono il **cambiamento dei processi operativi**, degli strumenti a supporto e la **formazione** del personale. La recente crisi ha aumentato la sensibilità verso la dematerializzazione

Culturali

- Il Digital Divide è tanto più ridotto quanto più i **processi digitali** sono **simili** a quelli **quotidiani** e quindi **naturali**. Ad es. l'adozione di scrivanie touchscreen per la lettura di un quotidiano a dimensioni reali

La firma digitale è già regolamentata dalla legge italiana

Firma Elettronica

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

Firma Elettronica Qualificata

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

Firma Digitale

- Particolare tipo di firma elettronica qualificata basata su un sistema di crittografia a chiave pubblica. E' la firma apposta con smart card o token rilasciato dal certificatore qualificato. In questo caso si sceglie una particolare tecnologia.

Firma Elettronica Avanzata

- Insieme di dati in forma elettronica allegati o connessi a un documento informatico che consentono l'identificazione del firmatario e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario conserva un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce, per permettere di rilevare se i dati stessi siano stati successivamente modificati.

CONTENUTI

- INTRODUZIONE: L' AZIENDA
- LA DEMATERIALIZZAZIONE
- LA FIRMA ELETTRONICA AVANZATA
- LA SOLUZIONE NAMIRIAL
- CONCLUSIONI

FIRMA ELETTRONICA AVANZATA - DEFINIZIONI

ART. 1 – CODICE AMMINISTRAZIONE DIGITALE
(DEFINIZIONI)

q-bis) 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;

ART. 56 – REGOLE TECNICHE
(CARATTERISTICHE DELLE SOLUZIONI DI FIRMA ELETTRONICA AVANZATA)

BOZZA

1. Le soluzioni di firma elettronica avanzata garantiscono:

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

ART. 58 – REGOLE TECNICHE
(SOGGETTI CHE REALIZZANO SOLUZIONI DI FIRMA ELETTRONICA AVANZATA A FAVORE DI TERZI)

1. I soggetti di cui all'articolo 55, comma 2, lettera b) che offrono una soluzione di firma elettronica avanzata alle pubbliche amministrazioni, **devono essere in possesso della certificazione di conformità** del proprio sistema di gestione per la sicurezza delle informazioni ad essi relative, 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

BOZZA

ART. 58 – REGOLE TECNICHE
(SOGGETTI CHE REALIZZANO SOLUZIONI DI FIRMA ELETTRONICA AVANZATA A FAVORE DI TERZI)

2. I soggetti di cui all'articolo 55, comma 2, lettera b) che offrono soluzioni di firma elettronica avanzata alle pubbliche amministrazioni, ovvero le società che li controllano, **devono essere in possesso della certificazione di conformità del proprio sistema di qualità alla norma ISO 9001** e successive modifiche o a norme equivalenti.

BUREAU VERITAS
Certification

Certificato di Conformità

Rilasciato a

NAMIRIAL SPA

SEDE LEGALE ED OPERATIVA:
Via Caduti Sul Lavoro, 4
60019 SENIGALLIA ()

Bureau Veritas Italia S.p.A. certifica che il Sistema di Gestione di questa organizzazione è stato valutato e giudicato conforme ai requisiti della norma

ISO 9001:2008

in relazione al seguente scopo

Progettazione, elaborazione ed assistenza post vendita di software, piattaforme gestionali e siti internet.
Erogazione di servizi hosting e collocation per centri di assistenza amministrativa e fiscale.
Erogazione del servizio di posta elettronica certificata.
Certification authority e time stamping.

Settore/i EA di attività 33

Data inizio validità 28/11/2007

BOZZA

CAD – Art. 21
(Valore probatorio del documento informatico sottoscritto)

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

2. **Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale**, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, **ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.**

3. 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.

Codice Civile
art. 2702

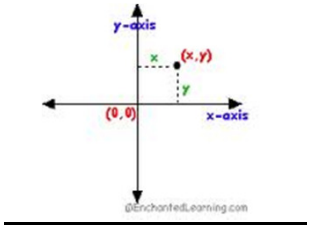
La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta.

INVERSIONE ONERE DELLA PROVA

La firma grafometrica

Tra le firme digitali, quella applicata su un dispositivo elettronico, in gergo tecnico «**firma grafometrica**», è quella che maggiormente consente di **ridurre l'effetto Digital Divide**, essendo la più vicina al processo naturale di firma di un documento cartaceo

La firma grafometrica è un particolare tipo di firma elettronica avanzata che si ottiene dal rilevamento dinamico dei dati calligrafici.
I dati rilevati per mezzo di una penna elettronica su una tavoletta digitale/schermo touchscreen sono:

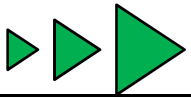


1. Posizione

2. Tempo

3. Pressione

Velocità



Accelerazione

La firma grafometrica consente di identificare in modo certo l'utente che firma e di ottimizzare il trattamento e l'archiviazione dei documenti firmati con risparmio di costi di gestione e miglioramento dei livelli di servizio

CONTENUTI

- INTRODUZIONE: L' AZIENDA
- LA DEMATERIALIZZAZIONE
- LA FIRMA ELETTRONICA AVANZATA
- LA SOLUZIONE NAMIRIAL
- CONCLUSIONI

La soluzione Namirial

La soluzione di Firma Grafometrica di Namirial S.p.A. è in realtà un **processo di Firma Elettronica Avanzata** denominato FirmaGrafoCerta che ha come prerogativa la presenza di una Certification Authority e la presenza di un operatore di front-end (professionista, operatore, impiegato ufficio etc…) che presiede all'atto della firma

Il processo **è certificato ISO 27001**, la norma internazionale che definisce i requisiti per impostare e gestire un Sistema di Gestione della Sicurezza delle Informazioni.

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

Studiata per gestire i documenti informatici nativi che prevedono l'apposizione di una o più firme autografe e per avere impatto minimo sugli utenti.

Elementi sistema: Software, dispositivi di firma

Connessione internet

Software ***Namirial FirmaCerta*** con abilitazione per la funzionalità di firmagrafometrica

Smart Card (Lettore opzionale) → soluzione più economica ma, nel caso di lettore, legata al terminale dove vanno installati sia i driver del lettore sia il software di firma.

Token USB → soluzione che garantisce la mobilità in quanto il software può essere installato direttamente sul dispositivo e non sul computer.

Firma da remoto su HSM → Soluzione che non richiede interazioni con il terminale ma che richiede dispositivi esterni di tipo OTP per l'apposizione del codice dinamico.

Approvigionamento di *marche temporali*

Elementi sistema: Hardware

Soluzioni per postazioni fisse

Tavolette LCD WACOM STU 520 / STU 500 – soluzioni (plug&play) – Le più economiche da connettere ad un terminale con Windows XP e superiori, ideale per postazioni di sportello.

Soluzioni per postazioni mobili

Tutte con Windows 7, si differenziano per le caratteristiche tecniche e per le periferiche; in comune hanno tutte lo schermo con rilevazione dell'indice pressorio, elemento obbligatorio per gestire la firma grafometrica.

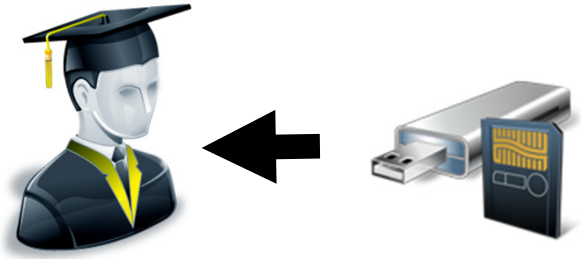
FUJITSU
STILISTIC Q550

Asus
Eee Slate B121

SAMSUNG
Serie 7 Slate PC

HP
EliteBook 2760p

Schema del processo FirmaGrafoCerta



Certification Authority

Formazione dell'operatore dell'ente con rilascio del dispositivo di firma digitale

Ente erogante il servizio

Prima identificazione del soggetto firmatario con firma dell'informativa sul servizio

Firma del documento elettronico (dati grafometrici firmatario + firma digitale RAO)

Caratteristiche FirmaGrafoCerta (1/3)

1. Con l'apposizione della firma digitale, l'operatore che riconosce viene responsabilizzato e contemporaneamente tutelato da eventuali sospetti;

2. Spariscono i concetti di falsi negativi e falsi negativi in quanto il processo di verifica è basato sul riconoscimento dell'operatore incaricato e non su confronti di firme;

3. Ad ogni firma corrisponde **una firma digitale e,** opzionale a seconda del documento, **una marcatura temporale**

4. Il documento emesso e sottoscritto è **autoconsistente**, contiene il dato biometrico crittografato che non può essere estratto e apposto su altri documenti.

5. 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.

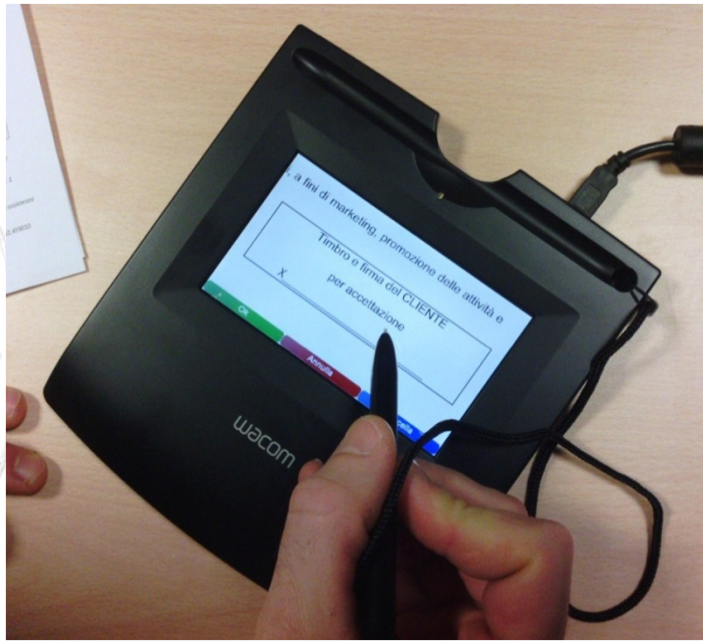
Caratteristiche FirmaGrafoCerta (2/3)

6. Sulla tablet viene mostrato il **dettaglio ingrandito del documento originale** per facilitare la comprensione di dove si sta firmando all'interlocutore (digital divide = zero)

7. Sulla tablet è anche possibile visualizzare l'intero documento navigando tra tutte le pagine, evitando quindi il dover sintetizzare documenti diversi da quelli originali.

8. E' disponibile uno strumento di creazione **template** per semplificare l'apposizione veloce di più firme su documenti con spazi fissi.

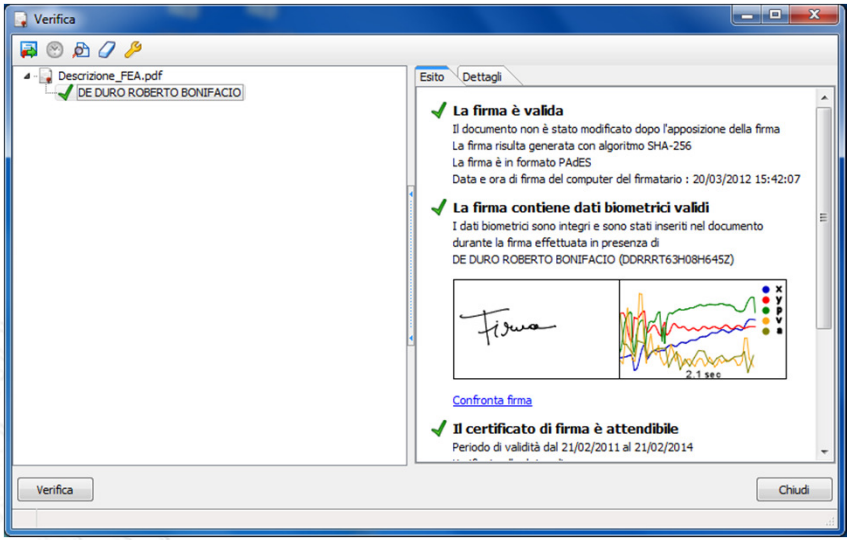
9. Ogni pagina contenente una firma viene marchiata per evidenziare che l'originale del documento non è cartaceo bensì digitale

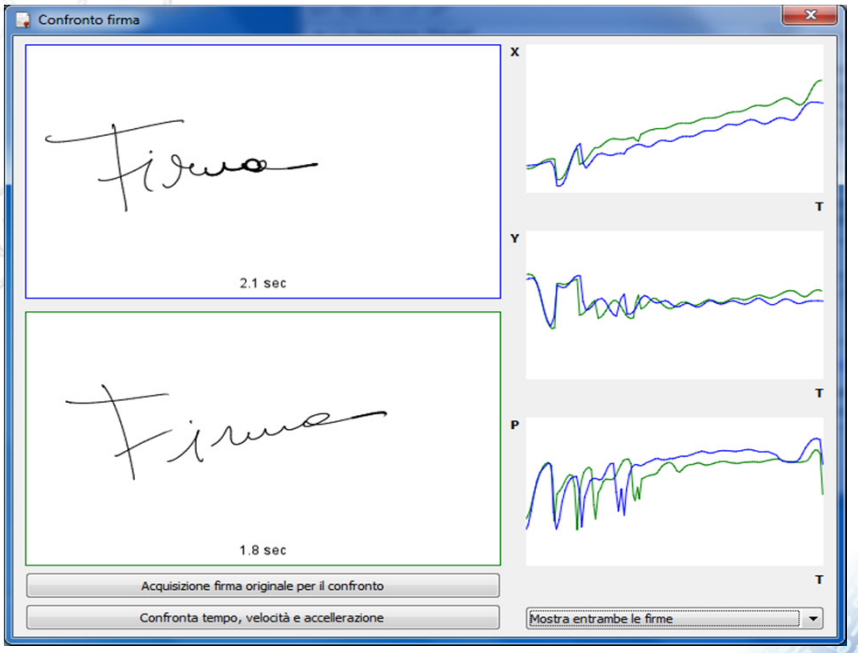


Caratteristiche FirmaGrafoCerta (3/3)

10. Per il controllo si utilizza uno strumento di **semplice confronto tra i dati biometrici** del soggetto firmatario presenti sul documento e quelli dello stesso rilevati contestualmente alla verifica. Lo strumento consente di estrarre i parametri in fase di perizia.

11. **Non si sfruttano algoritmi proprietari di verifica** che attualmente hanno una % di scarto che nel migliore delle ipotesi è del 4% e che non sono del tutto trasparenti nel loro funzionamento.





25

CONTENUTI

- INTRODUZIONE: L' AZIENDA
- LA DEMATERIALIZZAZIONE
- LA FIRMA ELETTRONICA AVANZATA
- LA SOLUZIONE NAMIRIAL
- CONCLUSIONI

FirmaGrafoCerta è la traduzione del flusso cartaceo……

FirmaGrafoCerta traduce il flusso cartaceo in digitale utilizzando strumenti riconosciuti dal Codice di Amministrazione Digitale:

- firma avanzata grafometrica del cliente;
- firma qualificata digitale dell'operatore che riconosce;
- marcatura temporale di Ente terzo che fornisce DataCerta;
- eventuale invio con Posta Elettronica Certificata;
- eventuale archiviazione con gestione della sostitutiva;

Questi componenti sono integrati secondo dei criteri tecnici ben precisi che sono stati oggetto della certificazione **ISO 27001**, la quale sarà obbligatoria secondo le regole tecniche in approvazione per una Pubblica Amministrazione che si vorrà dotare della soluzione.

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

...CON RIDUZIONE DEL RISCHIO.

Non aumenta il rischio di illeciti rispetto ad un flusso cartaceo perché lo ripropone. Infatti se un cliente disconosce la firma sul cartaceo lo può fare anche con il processo FirmaGrafoCerta con la differenza che deve provare anche che non era ne davanti all'operatore, che la ha riconosciuto firmando digitalmente, ne in quel determinato momento, identificato con la data certa della marcatura temporale.
Quindi il rischio in assoluto diminuisce.

In fase di contenzioso oggi il grafologo prende il documento (quando si trova) e lo studia; con FirmaGrafoCerta si estraggono i dati biometrici (decifrati in chiaro solo con intervento dell'Ente Terzo che detiene l'unica chiave privata) che contengono più informazioni rispetto a quelle presenti sul cartaceo (sia dati dinamici sia dati statici.

Rilasciata dalla Namirial in qualità di Autorità di Certificazione che ne garantisce la solidità, la validità e il corretto funzionamento (per utilizzi conformi al manuale operativo)

In sintesi

Soluzione software interamente **italiana**.

Processo certificato **ISO27001**

Garanzia di una **Autorità di Certificazione**

Soluzione completamente **integrabile**

Costo di integrazione **minimo**

Impatto zero sull'organizzazione e sui clienti