ISACA®

Sistemi informativi: averne fiducia e trarne valore

Rome Chapter

La firma biometrica:

Valore della firma biometrica nel nuovo scenario normativo sulle firme elettroniche

Carla Fazzi, CRISC
Valerio Cristofaro

Roma 02/07/2013

Presentazione dei relatori

Agenda

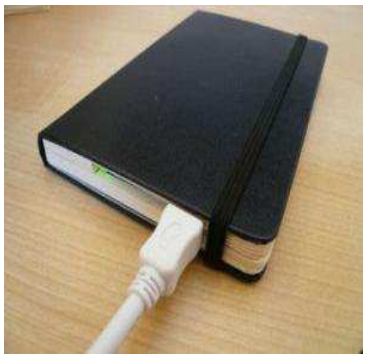
- Presentazione relatori
- La firma biometrica
  - Perché c'è interesse?
  - Terminologia
  - La firma grafometrica: caratteristiche
  - Gli standard
  - I Device
  - Le soluzioni e i Modelli di business
- Security & Compliance
  - Il documento informatico
  - Definizioni di firma elettronica
  - La grafometria
  - Gli aspetti di Sicurezza e Privacy

  Q&A
- Bibliografia & sitografia

Perché c’è interesse per la Firma Grafometrica?

- *"Most benefits attributed to any form of e-signature are really a result of automating a business process, and the signature is a small but important step in the process… E-signatures, including digital signatures, add efficiencies to formerly paper-based processes…" **

- *"Although the impact on commercial organizations is not significant at this point, the legal framework for digital signatures means that purchase orders and invoice systems using digital signatures are legally acceptable, and multiple implementations are in place in Germany..." ***

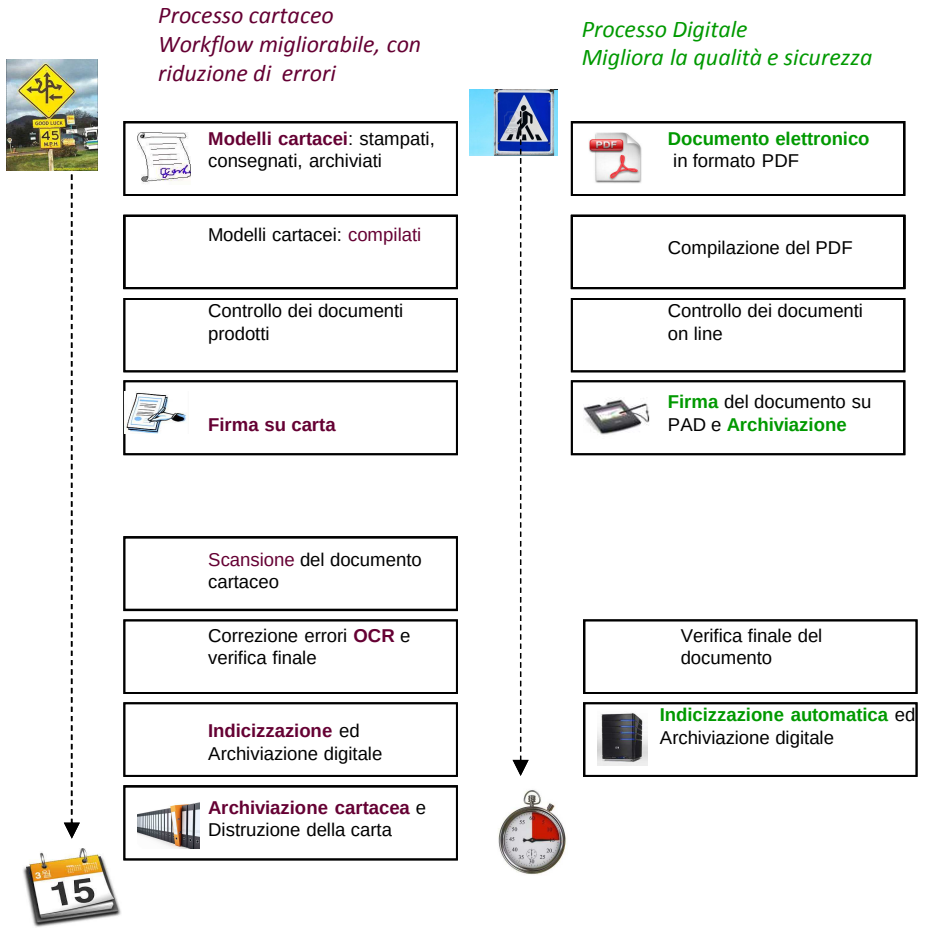


La novità è che oggi, grazie alla firma grafometrica, è addirittura possibile digitalizzare anche quei documenti e quei processi che fino a qualche tempo fa non era possibile dematerializzare, per questioni tecniche ma, soprattutto, per questioni normative.

* *(Gartner* ‘Hype Cycle for Governance, Risk and Compliance Technologies, 2008, by Gregg Kreizman, Carsten Casper and Kristen Noakes-Fry)
** *(*Gartner ‘Hype Cycle for Regulations and Related Standards, 2008’ by Gregg Kreizman, Carsten Casper and Kristen Noakes-Fry)

Quali sono i principali benefici?

- **Velocizza i processi (Workflow) di firma**
  - Riduzione tempi e costi di: stampa, invio, imbustamento, archiviazione dei documenti
  - Verifica automatica delle firme su chi possiede i diritti/deleghe di firma
  - Verifica/perizia della firma autografa grafometrica
- **Riduce i Costi**
  - workflow di gestione del documento più semplice
    - più sottoscrittori e firmano in sedi diverse
  - miglioramento della "service/user experiences
- **Combatte le Frodi**
  - Il fenomeno di transazioni fraudolente su Assegni e/o Transazioni Bancarie non accenna a decrescere e i numeri sono impressionanti
  - Il basso rischio di essere scoperti è verosimilmente la principale motivazione
- **Sicurezza**
  - I processi (o workflow) di *firma a "norma*" forniscono risposte veloci ed affidabili su chi ha firmato che cosa, dove e quando
  - Riduzione dei rischi operativi, specialmente in istituzioni finanziarie, autorità pubbliche e aziende private,
    - le banche o altre istituzioni finanziarie devono seguire le normative MiFID (Markets in Financial Instruments Directive) e di Antiriciclaggio (AML) e l'adozione di workflow di documentazione "sicuri" riduce l'esposizione ai rischi
- **Green Workflow**
  - La significativa riduzione di carta è un contributore per le strategie di Corporate Social Responsibility (CSR)



La firma Grafometrica: calligrafia o tecnologia?

- Rientra nelle tecnologie legate a quella branca chiamata biometria
- E' un particolare tipo di firma elettronica che si ottiene dal rilevamento dinamico dei dati calligrafici
  - ritmo, pressione, velocità, movimento della firma di un individuo che utilizza una penna elettronica per scrivere su una tavoletta (tablet) biometrica, cioé dotata di particolari sensori

Terminologia

Privacy

tablet

biometria

Certificato elettronico

archiviazione

ISO

Documento Informatico

Crittografia asimmetrica

security

enrollmentc

chiavi crittografiche

Firma elettronica semplice

La firma grafometrica

Firma elettronica

e-signature

pad

PEC

Firma elettronica qualificata

PKI

cifratura

integrità

PDF

Firma elettronica avanzata

certificato

standard

autenticazione

Firma Digitale

Firma autografa

compliance

policy

Conservazione Digitale

Garante

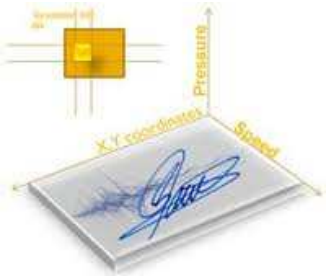
dematerializzazione

La firma grafometrica: caratteristiche

- Una "*caratteristica biometrica*" è un pattern unico di una caratteristica fisica di una persona come la retina, le impronte digitali, la voce o la grafia utilizzata per il riconoscimento di identità

  - La Firma Grafometrica è una caratteristica biometrica che utilizza le caratteristiche anatomiche e comportamentali di una persona durante la firma
    - è il risultato di una serie molto complessa di compiti neuromuscolari dinamici dal cervello alle dita

  - I software di firma autografa biometrica
    - consente di firmare i documenti attraverso il gesto naturale della mano apposto su un superficie dotata di tecnologia di rilevazione
    - si basa sulla tecnologia di riconoscimento grafometrico
      - sono in grado di catturare e comprende la dinamica della firma manoscritta della persona
      - utilizzano le caratteristiche anatomiche e comportamentali durante la firma

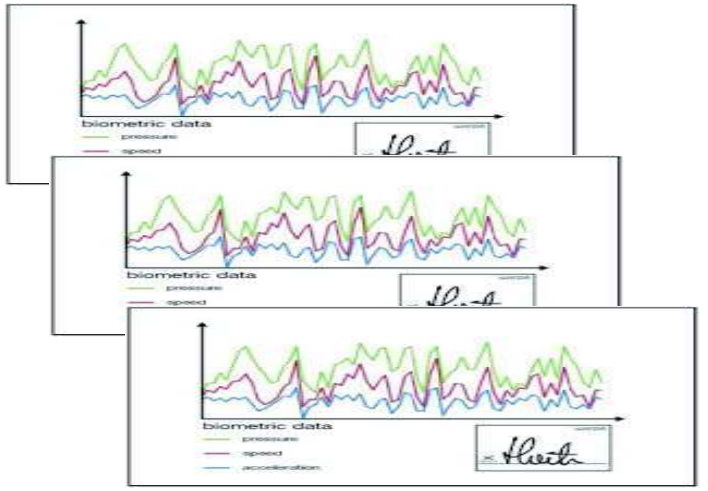


  - L'associazione univoca al firmatario avviene attraverso il riconoscimento di parametri statici e dinamici propri di ogni individuo (es. ritmo, velocità, pressione, accelerazione, movimento)

La firma grafometrica: firme dinamiche

Per capire ciò che è necessario per fidarsi di una firma, è importante tenere a mente che gli esperti forensi si basano su analisi olistica delle firme, cioè guardano e prendono in considerazione le caratteristiche della carta, il tipo di stilo, il flusso di inchiostro e la pressione visibile.

L'approccio olistico equivalente per le firme dinamiche deve tener conto di quale dispositivo è stato utilizzato per la cattura della firma, le caratteristiche del dispositivo e forse anche l'ambiente di firma e le co-relazioni per il processo di firma.



- Enrollment

Per ogni firmatario può essere creato un set di dati di riferimento unico che contiene informazioni sulle caratteristiche

  - dell'immagine statica della firma
  - segnali dinamici invisibili (biometrici) del movimento di scrittura come velocità e pressione, la posizione e il tempo

- Classificazione

La qualità del set di dati di riferimento è valutata durante l'enrollment e può essere regolata in base al device impiegato, ed ai livelli di sicurezza desiderati

- References o profiling

I dati relativi ai dati biometrici sono memorizzati come modelli su DB

Standard: ISO

- Biometric Signature Capturing Standard
  le regole in questa categoria sono rilevanti per permettere **interchanging data** di firma grafometrica

- Il formato di interscambio “Information technology — Biometric data interchange formats — Part 7: Signature/sign time series data” (19794-7:2005) considera i seguenti dati di serie temporali:
  - posizione penna orizzontale (ascisse),
  - posizione verticale penna (coordinate y),
  - altezza della penna di sopra del piano di scrittura (z-coordinate),
  - velocità in direzione x,
  - la velocità in direzione y,
  - l'accelerazione in direzione x,
  - l'accelerazione in direzione y,
  - la forza sulla punta della penna,
  - la punta della penna nel cambio tra tocco/non tocco il piano di scrittura,
  - l’ inclinazione della penna lungo l'asse x,
  - l’ inclinazione della penna lungo l'asse y,
  - azimut della penna,
  - l’ elevazione della penna,
  - la rotazione della penna.

  Lo standard ISO è un formato generico e può essere applicato e utilizzato in una vasta gamma di settori applicativi in cui sono coinvolti firme scritte a mano biometrici.

  .

- ISO/IEC 19794-7:2007 Biometric data interchange formats -- Part 7: Signature/sign time series data
- Da metà del 2012 è in corso di definizione una versione 19794-7 per XML

I device di firma: come sceglierli?

I device sono elemento fondamentale di un sistema di firma. I dispositivi di firma per essere considerati affidabili devono essere in grado di registrare sia le caratteristiche statiche e gli aspetti dinamici di una firma autografa.

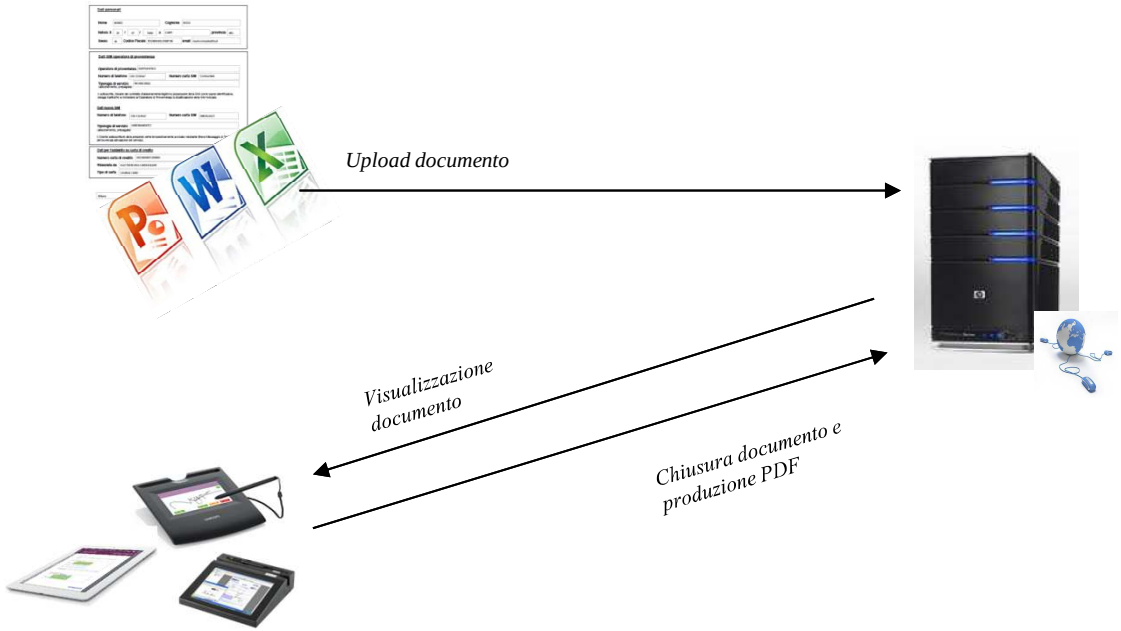
La scelta del dispositivo dipende dagli scenari di applicazione o di utilizzo:

- Pen Pad: consentono la firma su carta che è posizionata sulla parte superiore della tavoletta non-LCD
- Signature tablet: device dedicati che privilegiano la user-experience; possono essere mobile o per desktop
- Interactive Pen Display: device che permettono di navigare, annotare, e firmare i moduli elettronici e visualizzare i documenti migliorando la user-experience
- Kiosk system: hanno diverse caratteristiche aggiuntive a seconda delle esigenze della loro applicazione, ad esempio:
  - telecamere per catturare immagini
  - scanner di impronte digitali
  - passaporti o lettori di schede ID (per la zona a lettura ottica)
  - lettori di banda magnetica
- Tablet e tablet PCs: utilizzati prevalentemente in mobilità supportano modello di business complessi

Scenari di applicazione

Dematerializzazione all'origine dei documenti firmati

- ✓ Riduce drasticamente gli errori di data entry
- ✓ Velocizza l'intero processo, dalla compilazione dei campi del modulo, alla firma del Cliente, dall'invio del documento verso il Cliente, alla sua gestione e archiviazione in formato digitale
- ✓ L'intero processo avviene in assenza totale di carta



Le Soluzioni possono supportare diversi canali:

- Desktop: è il processo più semplice:
  - si apre il documento utilizzando sw di firma, si firma e immediatamente il documento è convertito in .pdf
  - si cattura la firma e i relativi dati biometrici, a cui si possono aggiungere "data certa" o altri strumenti di verifica
- Web Browser
  - Il documento è firmato e verificato tramite un browser web; pertanto si firma un viewer del documento
- Mobile
  - Può essere una soluzione ibrida fra Desktop e Web; in molti casi si installa un APP sul tablet o tablet PC che ha le stesse funzionalità del Web

Modelli di applicazione di Firma Grafometrica

- Firma Grafometrica
  - i dati della firma acquisita sono
    - associati *univocamente* al documento (in genere PDF) oggetto di sottoscrizione,
    - cifrati per renderli inaccessibili per un utilizzo con altri documenti,
    - inseriti in un normale campo di firma elettronica per proteggere l'integrità
  - la firma associata al documento è poi verificabile, in caso di disconoscimento, da parte di un grafologo che la esamina esattamente come nel caso cartaceo.

- Autenticazione basato sulla firma autografa - *Enrollment*
  - i dati della firma acquisita vengono confrontati con un database di "*specimen*" precedentemente raccolti.
  - Se il sistema riconosce una corrispondenza può abilitare una certa funzione (ad esempio un pagamento)

Firma Elettronica Grafometrica

Il processo di firma è gestito su un file PDF (formato PDF o PDF/A), e a valle della firma restituisce un file PDF con lo stesso nome ma con l'aggiunta dei dati biometrici e dei dati di firma

Acquisizione PDF

- Si apre il documento da firmare
- Il **completamento** del modulo può avvenire attraverso l'utilizzo della normale tastiera o, nel caso dei Tablet PC, della penna in dotazione
- Il **click** sul campo dedicato alla firma avvia il processo di sottoscrizione

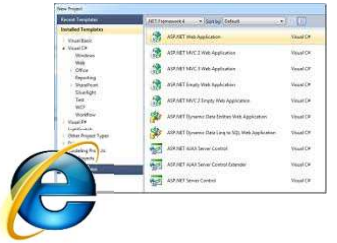
Firma

- Si appone la firma sul monitor del **PAD** o del **Tablet PC**
- Il **tratto grafometrico** viene cifrato e inserito all'interno del PDF
- Al PDF viene applicato un **certificato digitale**

Invio e archiviazione

- Il documento PDF viene trasferito tramite protocollo sicuro e archiviato nel **sistema documentale**

Visualizzazione



- Tramite un qualsiasi browser è possibile **accedere** al documento archiviato (anche in Conservazione Sostitutiva)

Metodo di Autenticazione basato sulla firma autografa

- *Enrollment*

Il processo di “raccolta di Firme di Campione” viene avviato con l’enrollment dell'utente.

Il processo di enrollment richiede fino a sei firme iniziali e può essere fatto continuamente nel tempo.

Le firme sono raccolte utilizzando un pad di firma o un tablet.

Le firme sono memorizzate nel db del cliente.

Il sistema può gestire numerosi profili per utente, permettendo, ad esempio, per un profilo di una firma standard ed un altro per la firma solo con le iniziali.

In fase di verifica di una firma, si confronta la firma apposta con il/i profili del cliente.

- **3. Verifica della Firma e Autoapprendimento**
- Ogni volta che un utente accede al sistema per verificare la sua firma, il sistema confronta la firma corrente ai profili di firma. Con ogni autenticazione, il server continua ad apprendere e perfezionare profilo dell'utente. Questo permette al sistema di tracciare cambiamenti graduali nel firma manoscritta nel tempo.

Funzionalità di Security e Compliance

- La comunicazione tra il dispositivo di firma e il PC avviene in modalità criptata
- Il documento firmato è archiviato in modalità criptata
- Il documento firmato non è più modificabile. Un certificato digitale ne garantisce l'integrità e l'inalterabilità, secondo gli standard di sicurezza
  - in caso di manomissione è lo stesso software PDF Reader a segnalare che il documento non è valido
- La firma grafometrica è protetta attraverso un sistema di crittografia asimmetrica
  - I dati di firma sono aggiunti al PDF e protetti con sistemi di public key encryption
  - In aggiunta alla firma autografa può essere utilizzato un sistema di chiavi esistente, come ad esempio USB token
- In caso di modifica attraverso software esterno il documento non è più riconosciuto come valido
- In qualche caso è possibile implementare Policy
  - disabilitare alcune funzionalità di un particolare documento, come ad esempio l'eliminazione di un campo firma predefinito
  - applicare le policy, come ad esempio la necessità di firmare i campi firma in un certo ordine
  - aggiungere un allegato con la fotocamera e così via

Agenda

- Presentazione relatori
- La firma biometrica
  - Perché c'è interesse?
  - Terminologia
  - La firma grafometrica: caratteristiche
  - Gli standard
  - I Device
  - Le soluzioni e i Modelli di business
- Security & Compliance
  - Il documento informatico
  - Definizioni di firma elettronica
  - La grafometria
  - Gli aspetti di Sicurezza e Privacy

  Q&A
- Bibliografia & sitografia

Il documento informatico

- **Legge Bassanini 15 marzo 1997:** "Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge" (art.15)

- **DPCM 8 febbraio 1999**: regole tecniche per la formazione, trasmissione, conservazione, duplicazione, riproduzione e validazione dei “documenti informatici”

- **DPR n°445 del 2000:** documenti informatici come “rappresentazione informatica di fatti, atti o dati giuridicamente rilevanti”

- **D.lgs 23 gennaio 2002, n°10** (assorbito, con alcune integrazioni, dal D.lgs 7 marzo 2005, n°82): recepimento disposizioni europee sulla firma elettronica

Le firme elettroniche: la Direttiva 1999/93/CE

- **Firma Elettronica Semplice**

  Un metodo informatico di autenticazione

- **Firma Elettronica Avanzata**

  Una sottoscrizione autografa estremamente complessa in grado di garantire:
  - la connessione univoca al firmatario
  - la sua identificazione
  - il controllo esclusivo sul mezzo necessario a crearla
  - l'identificazione di ogni successiva modifica del documento a cui fosse associata

La Firma Elettronica Avanzata: tra passato e futuro

Il recepimento delle disposizioni europee demandata al D. lgs. 23 gennaio 2002 n°10 ha visto il recepimento nell'ordinamento italiano della solo Firma Elettronica e della c.d. Firma Elettronica Qualificata (comprensiva della Firma Digitale).

Il "ritorno" della Firma Elettronica Avanzata, come quarta fattispecie, è stato sancito dalle modifiche introdotte dal D. lgs. 30 dicembre 2010 n°235 e si è completato con la pubblicazione del **DPCM del 22 Febbraio 2013** (Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali).

Tipologie di firma: La Firma Elettronica

- **Caratteristiche**

  Un insieme di dati in forma elettronica allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di identificazione informatica

- **Valore**:
  - il documento sottoscritto sarà riconosciuto dall'ordinamento come forma scritta quando garantisca in modo oggettivo qualità, integrità, sicurezza e immodificabilità
  - efficacia probatoria liberamente valutata dal giudice
  - scarse garanzie in termini di opponibilità ai terzi

- **Casi d'uso**

  15° Censimento Nazionale della Popolazione e delle Abitazioni: il cittadino ha potuto autenticarsi al portale ISTAT per la compilazione del modulo, identificandosi tramite Codice Fiscale e password (riportata all'interno del documento cartaceo ricevuto presso il domicilio)

Tipologie di firma: La Firma Elettronica Qualificata

- **Caratteristiche**

  E' un tipo di firma elettronica avanzata che consente una stretta connessione tra l'oggetto sottoscritto e la firma, per il tramite:

  - di un dispositivo sicuro
  - un "certificato qualificato" rilasciato da un ente certificatore (attestato elettronico che collega all'identità del titolare i dati utilizzati per verificare la firma)

- **Valore**
  - Al documento sottoscritto è riconosciuta piena efficacia probatoria (forma scritta e sottoscritta)

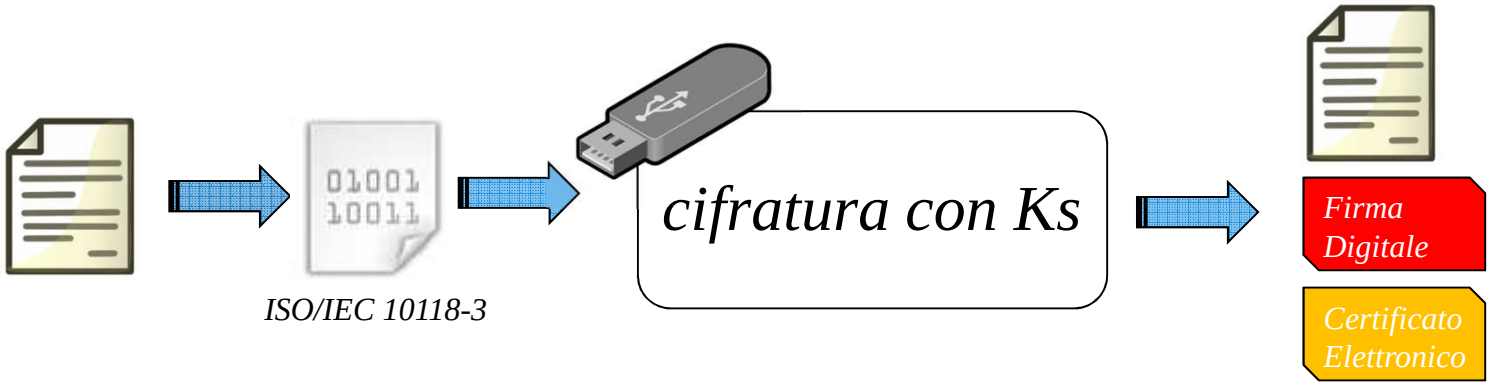
Il tipo di Firma Elettronica Qualificata più utilizzato in Italia è la **Firma Digitale**

Tipologie di firma: La Firma Digitale

- **Caratteristiche**

  E’ un tipo di Firma Elettronica Qualificata basato su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consentono di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici

  Sotto il profilo pratico essa è il risultato di un algoritmo crittografico a chiavi asimmetriche, di lunghezza minima 1024 bit, applicato all’impronta digitale del file contenente la rappresentazione del documento



ISO/IEC 10118-3

Tipologie di firma: La Firma Digitale 2/2

- **Valore**

  Lo stesso della firma elettronica qualificata

- **Casi d'uso**

  procedura di deposito del bilancio presso il Registro delle Imprese, che prevede la sottoscrizione digitale della pratica da parte del legale rappresentante

Tipologie di firma: La Firma Elettronica Avanzata

- **Caratteristiche**
  - identificazione del firmatario
  - connessione univoca della firma al firmatario
  - controllo esclusivo del firmatario sul sistema di generazione della firma
  - immodificabilità del documento
  - possibilità per il firmatario di ottenere evidenza di quanto sottoscritto
  - individuazione del soggetto che eroga le soluzioni di firma elettronica avanzata

- **Valore**

  Efficacia probatoria prevista dall'art. 2702 del codice civile per la scrittura privata. L'unica eccezione è rappresentata dai casi previsti dall'art. 1350

- **Casi d'uso**
  - Invio tramite PEC
  - Utilizzo della Carta d'Identità Elettronica

Da strumento a processo

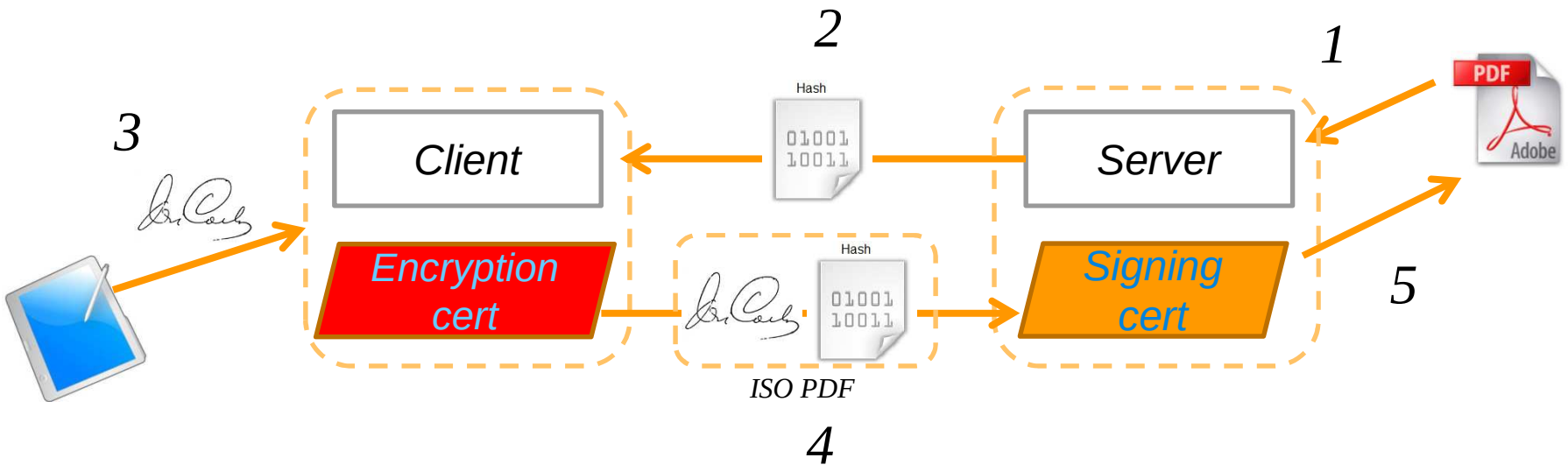
- **Neutralità tecnologica**

- **Requisiti soggettivi**
  - utilizzo esclusivo nei rapporti giuridici intercorrenti tra il sottoscrittore ed il soggetto che utilizza la soluzione di firma
  - identificazione certa dell'utente e obbligo di informativa sui termini e sulle condizioni relative all'uso del servizio, compresa ogni eventuale limitazione.
  - sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente (conservazione ventennale)
  - previsione dell'uso alternativo, ove applicabile, della Firma Elettronica Qualificata e della Firma Digitale
  - previsione di un servizio di revoca e di un servizio di assistenza
  - responsabilità dei soggetti che realizzano direttamente tali soluzioni per eventuali danni derivanti dall'attività svolta per almeno seicentomila euro

La firma grafometrica: quale firma ?

- Le tavolette sono in grado di registrare i parametri biometrici e di memorizzarli in un *template biometrico* di un paio di Kbyte circa. La connessione univoca della firma al firmatario è garantita dall'unicità dei dati biometrici memorizzati, univocamente associati a quell'unico sottoscrittore (art. 56 DPCM 22 Febbraio 2013)

- Il template viene utilizzato come dato per la creazione della firma e viene incorporato all'interno del documento



Vulnerabilità e scenari di mitigazione

- Intercettazione del dato biometrico nella comunicazione tra la tablet, client e componente server
- Lettura non autorizzata dei dati biometrici registrati sul client
- Utilizzo dei dati biometrici in un documento differente da quello che si sta firmando (o in posizioni differenti)
- Dialogo tra client e server fittizi
- Estrazione del pacchetto dei dati biometrici e decifratura del suo contenuto
- Manomissioni del PAD a scopo fraudolento
- Sostituzione di alcune componenti software con oggetti equivalenti, ma opportunamente modificati

Dato biometrico e Garante Privacy

La normativa italiana in materia di protezione dati personali consente il trattamento dei dati biometrici solo se vengono rispettate una serie di misure organizzative, tecniche e di sicurezza.

Documento di Lavoro sulla Biometria adottato in data 1° agosto 2003 dal Gruppo europeo per la tutela dei dati personali nelle due versioni di:

- Linee Guida in materia di trattamento di dati personali dei lavoratori privati e pubblici
- Decalogo su corpo e privacy

Decalogo su corpo e privacy

1. Affidabilità del sistema di rilevazione (indicazione del livello di accuratezza e della rigorosità dei controlli)
2. Informativa chiara con piena libertà di aderire o meno al sistema
3. Liceità verificabile sotto i profili di necessità, proporzionalità, finalità, correttezza, adeguatezza e qualità dei dati
4. Deroga motivata con uso controllato in speciali casistiche e non uso generalizzato o incontrollato o indifferenziato (riesame periodico)
5. Delimitata memorizzazione e non centralizzazione, anche se con dati cifrati.
6. Temporanea conservazione per il necessario periodo limitato
7. Scrupolose misure di sicurezza
8. Piena ed immediata conoscibilità dei dati biometrici da parte dell'interessato
9. Rispetto rigoroso degli obblighi di verifica preliminare e di notifica
10. Disattivazione automatica, immediata e certa di funzioni di smart card o altre analoghe nel caso di smarrimento o di furto.

Provvedimenti del Garante

- **Provvedimento n°36 del 31 gennaio 2013** (Cassa di Risparmio Parma e Piacenza)

- **Provvedimento Garante n°37 del 31 gennaio 2013** (Unicredit):

Presupposti di liceità e di finalità:

- identificare rigorosamente la clientela in occasione dello svolgimento delle operazioni bancarie (d.lgs. n. 231/2007, anti-riciclaggio)
- sviluppare una serie di vantaggi a beneficio della clientela;
- maggiore sicurezza contro i tentativi di frode;
- riduzione dei rischi di furto di identità e contraffazione della firma (prevenendo il rischio di smarrimento di strumenti quali smart card, token usb ecc.).

Q&A

Sitografia

Standard ISO: ISO/IEC 19794-7:2007 Biometric data interchange formats -- Part 7: Signature/sign time series data

Gartner. www.gartner.com

Namirial: http://www.firmagrafometrica.it/index.asp

Xyzmo: http://www.xyzmo.com/en/Pages/xyzmostart.aspx

Softpro: http://www.softpro.de/en/

Wacom: http://www.wacom.com/

Bibliografia

“ Guida Pratica su Firme Elettroniche e Firme Grafometriche”, Studio Legale Lisi, www.studiolegalelisi.it

“La normativa sulla firma elettronica”, Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA)

“Il nuovo CAD. Commenti e prospettive”, Minigrafia n°9, Fondazione Siav Academy

“Brevi note sulle tecnologie biometriche in un contesto ICT”, Gruppo di studio per la definizione di iniziative nel campo della biometrica (CNIPA), Gennaio 2004

“Linee guida per l'impiego delle tecnologie biometriche nelle Pubbliche Amministrazioni”, I Quaderni, n°9, Anno I - Novembre 2004, Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA)

“ Sistemi di Firma Biometrica”, Valerio Cristofaro, Università degli studi di Macerata

Contatti

- carlafazzi@libero.it
- valerio.cristofaro@postel.it

Grazie...

ISACA
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter