Relazione tecnica per la soluzione di firma grafometrica di Consultinvest Investimenti SIM SpA

Indice

Introduzione 3

Normativa di riferimento 3

Soggetto che eroga la soluzione 3

Soggetto che realizza la soluzione 4

Finalità dell'adozione della soluzione 5

Obblighi e responsabilità di Consultinvest Investimenti SIM SpA 5

Il processo di identificazione e firma adottato 7

Caratteristiche della soluzione 8

Scenari di utilizzo 8

Le tecnologie utilizzate dalla soluzione di firma 9

Dispositivi adottati 9

Aspetti organizzativi 10

Modalità di adesione al Servizio 10

Disponibilità dei documenti sottoscritti dal Cliente 10

Revoca del servizio di FEA 10

Disponibilità di sistemi alternativi 10

Protezione dei sistemi informatici e dei Client 11

Processo di acquisizione delle firme 12

Sicurezza del vettore biometrico 14

Protezione del dato biometrico sul dispositivo 15

Strutture dati per la protezione dei dati grafometrici 16

Struttura del vettore biometrico 16

Struttura del dizionario di firma pdf 17

Estrazione dei dati grafometrici e verifica delle firme 21

Procedura di verifica e perizia calligrafica 21

Caratteristiche della generazione dei certificati di cifra 23

Generazione a mezzo della CA del Notariato 23

Consegna e conservazione della chiave privata 23

Cenni professionali del Notaio incaricato 25

Recapiti 25

Processo di conservazione digitale dei documenti 26

Introduzione

La presente relazione:

- descrive gli aspetti tecnici e organizzativi delle misure messe in atto da Consultinvest Investimenti SIM SpA, in quanto titolare del trattamento di dati biometrici mediante un sistema di firma grafometrica posto al base di una soluzione di firma elettronica avanzata, così come definita dal Decreto Legislativo 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale" che non prevedono la conservazione centralizzata di dati biometrici.
- fornisce la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alla finalità di sottoscrizione di modulistica quali Raccomandazioni, Moduli Attestazione Ordini (MAO) e prima sottoscrizione tra i clienti e Consultinvest Investimenti SIM SpA.

Questa relazione tecnica è conservata aggiornata, con verifica di controllo annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione dell'Autorità Garante per la Protezione dei Dati Personali.

Normativa di riferimento

La soluzione è stata realizzata in ottemperanza a quanto previsto da:

- CODICE DELL'AMMINISTRAZIONE DIGITALE
  CAD - Decreto Legislativo 7 marzo 2005, n. 82
  http://archivio.digitpa.gov.it/amministrazione-digitale/CAD-testo-vigente

- DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 22 FEBBRAIO 2013
  Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali
  http://www.gazzettaufficiale.it/eli/id/2013/05/21/13A04284/sg

- PROVVEDIMENTO GENERALE 513 PRESCRITTIVO IN TEMA DI BIOMETRIA - 12 NOVEMBRE 2014
  http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3556992
  - All A al Provv. 513 del 12 novembre 2014 - Linee-guida biometria.pdf
    http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3563006
  - All B al Provv. 513 del 12 novembre 2014 Mod. segnalazione data breach.pdf
    http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3563019

e successive modifiche/integrazioni.

Soggetto che eroga la soluzione

Consultinvest Investimenti SIM SpA eroga la soluzione di FEA di tipo grafometrico avvalendosi della società Unimatica S.p.A. che realizza soluzioni di FEA anche di tipo grafometrico. In particolare Consultinvest Investimenti SIM SpA utilizza la piattaforma di firma elettronica UNISERV ed i servizi di conservazione digitale UNISTORAGE.

Soggetto che realizza la soluzione

La società Unimatica Spa che ha realizzato le componenti utilizzate per l'erogazione del servizio è in possesso delle certificazioni di qualità (UNI EN ISO-9001;2008), di sicurezza (ISO/IEC 27001) specifiche per l'erogazione dei servizi in oggetto ed è iscritta nell'elenco dei certificatori conservatori dell'Agenzia per l'Italia Digitale (AgID) e quindi abilitata a svolgere servizi di conservazione digitale a norma in ottemperanza alle vigenti regole tecniche in materia.

Finalità dell'adozione della soluzione

La finalità dell'adozione della soluzione di Firma Elettronica Avanzata è la semplificazione del processo di sottoscrizione di documenti che stanno alla base dei rapporti tra i clienti (soggetti firmatari) e CLIENTE attraverso la dematerializzazione documentale e la raccolta del dato biometrico.

I documenti informatici sottoscritti con firma grafometrica hanno la stessa validità ed efficacia probatoria dell'atto di scrittura privata, così come disciplinato dal Codice Civile, art.2702 (nota 3):

> *(3) Valore di scrittura privata riconosciuta è stato attribuito anche al documento informatico sottoscritto con firma elettronica nel rispetto delle regole tecniche che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento. L'art. 15, comma 2, della L. 59/97 (Bassanini) ha conferito infatti al documento informatico la medesima validità e rilevanza giuridica degli atti redatti su supporto cartaceo, e successivamente il d. P. R. 28 dicembre 2000, n. 445 ha confermato tale principio decisamente innovativo per il nostro ordinamento, sancendone la validità a tutti gli effetti di legge, sia sotto il profilo della validità, sia sotto il profilo dell'efficacia probatoria. L'unica condizione richiesta è l'osservanza delle disposizioni del decreto, le quali hanno prescritto la necessità della firma digitale e di una serie di complessi requisiti tecnici, in grado di garantire in maniera univoca provenienza e integrità del documento informatico. L'art. 10 dello stesso decreto stabilisce poi l'estensione delle disposizioni dell'art. 2712 al documento informatico, attribuendogli quindi la possibilità di formare piena prova in ordine alle cose e ai fatti in esso rappresentate, sempre che la parte contro cui sono prodotte non le disconosca.*

La soluzione adottata da Consultinvest Investimenti SIM SpA raccoglie i dati di natura biometrica (coordinate spaziali nel tempo) pertinenti alle firme apposte tramite dispositivi per la sottoscrizione di documenti elettronici nell'ambito dei rapporti intrattenuti tra il cliente e Consultinvest Investimenti SIM SpA ai fini di attribuire alla sottoscrizione gli effetti di una firma elettronica avanzata secondo quanto stabilito dal Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005) e dalle Regole Tecniche. Tale finalità viene descritta nell'informativa messa a disposizione del cliente. I dati biometrici raccolti non sono oggetto di diffusione.

Obblighi e responsabilità di Consultinvest Investimenti SIM SpA

Il processo adottato da Consultinvest Investimenti SIM SpA è qualificato come FEA – Firma Elettronica Avanzata e, pertanto, la normativa richiede al cliente che sceglie di aderire al servizio di sottoscrizione con firma grafometrica di documenti e/o contratti di accettarne espressamente le relative condizioni di utilizzo.

Consultinvest Investimenti SIM SpA, in qualità di soggetto che eroga la soluzione di FEA è responsabile verso il cliente per l'adempimento di tutti gli obblighi discendenti dall'espletamento di tale attività. In particolare è tenuta al rispetto

- di quanto previsto in tema di requisiti tecnici, procedurali ed organizzativi previsti dal CAD e dalle Regole Tecniche
- dei presupposti di legittimità contenuti nel Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003, n. 196 e nelle Linee-guida in materia di riconoscimento biometrico e firma grafometrica (Allegato A al Provvedimento del Garante del 12 novembre 2014)

e che vengano adottate tutte le misure e gli accorgimenti tecnici descritti nel Provvedimento del Garante del 12 novembre 2014.

Nell'interesse del cliente ed in ottemperanza a quanto previsto dal comma 2 dell'art. 57 del DPCM 22 febbraio 2013, Consultinvest Investimenti SIM SpA *ha stipulato una polizza assicurativa per la responsabilità civile da danno a terzi eventualmente derivante dalla fornitura del servizio di Firma Elettronica Avanzata rilasciata da* Generali Italia S.p.A. Il cliente, a seguito dell'adesione al servizio di FEA che si concretizza con l'atto di sottoscrizione della modulistica di adesione predisposta, riceve l'informativa per l'adesione al servizio con la descrizione delle caratteristiche tecniche e organizzative della soluzione di Firma elettronica avanzata adottata. La modulistica di adesione e le informative vengono opportunamente conservate e rimangono a disposizione del cliente anche attraverso il sito internet di Consultinvest Investimenti SIM SpA.

Il Garante ha inserito nel registro dei trattamenti la notifica di Consultinvest Investimenti SIM SpA. Tale notifica è accessibile all'URL http://www.garanteprivacy.it/ . Le notizie accessibili tramite la consultazione del registro possono essere trattate per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali.

Il processo di identificazione e firma adottato

Consultinvest Investimenti SIM SpA al fine di rispettare gli obblighi previsti dall'art. 56 del DCPM 22/02/2013 (consultabile all'url seguente: http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/dpcm_22_febbraio_2013_nuove_regole_tecniche.pdf in cui sono definite le caratteristiche delle soluzioni di firma elettronica avanzata) ha adottato le seguenti misure:

a) i consulenti finanziari di Consultinvest Investimenti SIM SpA :
- accertano "de visu" l'identità dei soggetti firmatari mediante un documento di riconoscimento in corso di validità ai sensi dell'art. 35 del DPR 445/2000;
- informano in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso;
- richiedono la sottoscrizione della dichiarazione di accettazione e informativa ex art.13 del D.Lgs.196 del 30 giugno 2003, per l'adesione al servizio.

b) la connessione univoca della firma al firmatario viene garantita mediante il prelievo dei dati biometrici, associati univocamente al soggetto che esegue il tratto di firma che, in forma crittata (mediante algoritmi a chiave asimmetrica) e insieme all'impronta del documento sono concatenati al documento output del processo di firma.

c) Il firmatario ha il controllo esclusivo del sistema di generazione della firma, avendo sempre la possibilità di:
- Visualizzare il documento
- Apporre la firma
- Annullare la firma apposta e ripetere la firma
- Annullare l'operazione di firma

d) Il firmatario ha sempre la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma.
Presso AgID all' URL http://www.agid.gov.it/identita-digitali/firme-elettroniche/software-verifica, sono disponibili, gratuitamente, una serie di software conformi alla Deliberazione N. 45 del 21 maggio 2009. Anche Adobe Acrobat Reader® è in grato di eseguire la verifica.

e) Il firmatario ha sempre evidenza di quanto sottoscrive perché sul dispositivo di firma o sul video messo a disposizione dal consulente Finanziario è visualizzato il documento; inoltre potrà richiedere la stampa del documento originale oltre al fatto che l'invio dello stesso avviene tramite PEC sull'email indicata dal cliente per il recapito della documentazione.

f) Il firmatario è sempre in grado di identificare con certezza Consultinvest Investimenti SIM SpA (come soggetto che eroga la soluzione di firma), in quanto l'applicativo è integrato nel sistema di front end in uso dalla rete dei consulenti finanziari che riporta in evidenza il logo della società, così come su tutti i documenti (ad e. Raccomandazione e MAO).

g) L'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati dallo standard con cui sono prodotti i documenti, che sono in formato PDF in assenza di link a risorse esterne e macro che potrebbero alterare il contenuto informativo e non modificabili successivamente all'atto della firma, a meno di una definitiva corruzione della validità della firma stessa.

h) La connessione univoca della firma al documento sottoscritto è garantita dalla Soluzione di FEA attraverso una procedura definita "document binding" in grado di dimostrare in maniera

inequivocabile la correlazione fra il documento e la firma apposta sulla tavoletta – ottenuta collegando immediatamente l'hash del documento ed i dati biometrici cifrati nell'applicativo client.

Il rispetto dei requisiti sopra descritti, enunciati nell'art.56 delle Regole Tecniche DCPM 22/02/2013, garantisce anche il rispetto di quanto disposto dall'Art.21 comma 2-bis del CAD.

Caratteristiche della soluzione

La soluzione di firma adottata da Consultinvest Investimenti SIM SpA si concretizza mediante la piattaforma di firma elettronica UNISERV di Unimatica Spa.

La piattaforma Uniserv è composta da:

- **una componente Client** che viene attivata dal browser della postazione di lavoro dell' operatore, tramite la quale viene reso disponibile il documento in formato grafico e ottimizzato, da sottoporre alla consultazione ed alla firma del cliente
- **una componente Server** installata presso la Server Farm di Unimatica, in cui risiede il documento originale, che comunica per l'intero processo con la componente Client.

La componente Client di Firma, dopo aver acquisito i dati biometrici dal dispositivo di firma, invia una serie di dati, tutti cifrati, tra cui il tratto grafico, il vettore biometrico e la chiave crittografica (AES) al Server di firma, il quale inserisce i dati ricevuti nel documento, ed invia al Client di Firma l'esito positivo dell'inserimento della firma con il nuovo HASH dello stesso per eventuali altre firme.

A seguito della conferma inviata mediante il Client di Firma della conclusione delle operazioni di sottoscrizione, il Server di Firma appone la firma elettronica dell'operatore di Consultinvest Investimenti SIM SpA e sigilla il documento con la firma elettronica qualificata di Consultinvest Investimenti SIM SpA, a garanzia di integrità e autenticità dello stesso. La firma elettronica avanzata è in standard PAdES secondo la deliberazione CNIPA 21 maggio 2009, n.45. A seguito della conferma inviata mediante il Client di Firma del completamento delle operazioni di sottoscrizione, il Server di Firma conclude il processo e restituisce il documento firmato.

Al termine del processo, i dati in memoria, relativi alla firma dei documenti residenti della postazione di lavoro dell'operatore della Compagnia vengono cancellati.

Il sistema descritto da una parte acquisisce dati personali comportamentali, riconducibili alla biometria, dall'altra prevede che tali dati non siano nella disponibilità del soggetto che li detiene, né la possibilità di essere estratti o duplicati, dando un altissimo livello di sicurezza al processo di firma.

Scenari di utilizzo

Il Cliente ha la possibilità di utilizzare il servizio di firma grafometrica per dare corso all'esecuzione della principale operatività presente in Consultinvest Investimenti SIM SpA. A titolo di esempio può firmare in formato grafometrico, ricevendo poi tramite PEC copia di tutta la documentazione, la raccomandazione di portafoglio, il modulo per l'operatività relativa all'investimento effettuato, i moduli di prima sottoscrizione dei prodotti finanziari collocati dalla Consultinvest Investimenti SIM SpA.

Le tecnologie utilizzate dalla soluzione di firma

La soluzione di firma richiede l'utilizzo di strumenti a supporto per l'apposizione della firma e per il corretto funzionamento.

Componenti Hardware e Software e integrazione

La soluzione di firma grafometrica adottata richiede l'utilizzo:

- del browser installato sul device in uso alla rete dei consulenti finanziari di Consultinvest Investimenti SIM SpA, configurato in modo tale da garantire un corretto colloquio Client-Server
- del Client di Firma che esegue le operazioni in un ambiente protetto, dialogando con il dispositivo di firma ed il Server di Firma su canali cifrati,
- del Server di Firma che riceve il documento in formato PDF, lo trasforma in immagine ottimizzata, lo invia al Client di Firma, gestisce la comunicazione con il Client, inserisce il vettore biometrico cifrato nel documento PDF, fino alla firma del documento stesso.
- del Server di Conservazione che riceve il documento completo con i vettori biometrici e, dopo averne verificata l'integrità ed autenticità, attiva il processo di conservazione. Il Server di conservazione permetterà di ottenere copia del documento corredata delle evidenze di conservazione per tutto il periodo definito. Inoltre consentirà di ricercare il documento per mezzo dei metadati associati e di produrne altre copie prive dei vettori biometrici ("flat") anche nel futuro.
- dei Server su cui risiede il sistema gestionale della Consultinvest Investimenti SIM SpA, dove viene tracciata ogni singola azione relativa al processo di firma

Dispositivi adottati

I dispositivi di firma adottati dalla Consultinvest Investimenti SIM SpA sono:

- Tablet Samsung modello è Galaxy Note 10.1
- Tablet Samsung modello è Galaxy Note 10.1 2014 Edition

Il tablet, dispositivo mobile, riceve e visualizza l'immagine ottimizzata dei documenti da sottoscrivere. I sensori del display rilevano tramite la penna elettronica la pressione esercitata, i punti della penna rilevati sul display e la velocità e individuano un unico profilo biometrico della firma, rendendo praticamente impossibile qualsiasi tentativo di riproduzione illecita.

Aspetti organizzativi

Modalità di adesione al Servizio

Come anticipato, il processo di adesione di un Cliente al Servizio di FEA (Firma Grafometrica) ha carattere "**una tantum**" nel rapporto con il cliente, ed il suo svolgimento è previsto solo funzionalmente all'effettivo utilizzo della Firma Grafometrica stessa.

Per l'adesione al Servizio di Firma Elettronica Avanzata, il Gestore è tenuto al **riconoscimento cliente** mediante verifica del documento di identità in corso di validità, di cui deve acquisire una copia.

Disponibilità dei documenti sottoscritti dal Cliente

Consultinvest Investimenti SIM SpA fornisce, liberamente e gratuitamente, al cliente firmatario, copia dei documenti descritti; tali documenti vengono inviati, al termine del processo di firma e di verifica dell'operazione, tramite PEC *(*servizio.contratti@pec.consultinvest.it *)* ad hoc attivata da Consultinvest Investimenti SIM SpA. L'email destinataria è quella indicata dal Cliente firmatario all'atto dell'adesione al servizio di Firma Grafometrica. In copia conoscenza di tutti gli invii documentali è inserito il Consulente Finanziario.

I documenti firmati potranno essere richiesti direttamente al Consulente Finanziario o all'Assistenza Clienti di Consultinvest Investimenti SIM SpA tramite richiesta scritta allegando copia del documento di identità.

Il cliente riceve copia cartacea della sottoscrizione della dichiarazione di accettazione e l'Informativa ex art. 13 direttamente dal Consulente Finanziario all'atto dell'adesione al servizio (firmando il modulo denominato " Termini e condizioni del servizio di firma elettronica avanzata e Informativa preliminare ai sensi dell'art. 13 del D.Lgs. 196/2003 (Codice di Tutela dei Dati Personali").
Riceverà invece via email tutti i documenti contrattuali sottoscritti con la FEA.

Revoca del servizio di FEA

Il cliente può, in ogni momento, richiedere la revoca all'utilizzo del servizio di Firma Elettronica Avanzata adottato da Consultinvest Investimenti SIM SpA compilando una "Richiesta di revoca dal servizio di Firma Elettronica Avanzata" disponibile per il tramite del Consulente Finanziario o all'Assistenza Clienti di Consultinvest Investimenti SIM SpA.

Disponibilità di sistemi alternativi

In caso di revoca da parte del cliente dal Servizio di Firma Elettronica Avanzata (o di non sottoscrizione del Servizio stesso), l'operatività del cliente con Consultinvest Investimenti SIM SpA è garantita tramite modalità alternative cartacee di sottoscrizione che non prevedono la raccolta di dati biometrici.

Protezione dei sistemi informatici e dei Client

In questa sezione vengono documentare le misure di sicurezza messe in atto da Consultinvest Investimenti SIM SpA sui propri sistemi a garanzia della protezione dei dati personali che vengono trattati all'interno del processo. Oltre all'utilizzo di un sistema MDM, anche in ottemperanza di quanto richiesto dal provvedimento del garante della privacy, in caso di mobilità e il dettaglio di DATA BREACHES.

Vengono, infatti, adottati sistemi di firewall hardware Cisco ASA in failover, al fine di proteggere la rete locale da accessi non autorizzati, con mascheramento NAT degli indirizzi IP dei client della rete che si collegano ad Internet.

Le porte TCP/UDP sono tutte chiuse tranne quelle strettamente necessarie all'operatività della società

Vengono altresì adottati sistemi antivirus e filtri antispam server/client centralizzati Kaspersky Enterprise e Symantec Enterprise, con protezione attiva in tempo reale, verifica di tutti i file richiamati per esecuzione, per modifica, per copia, per backup; verifica la posta elettronica e gli allegati in ingresso. Le definizioni dei virus sono aggiornate automaticamente ogni ora. I server, sui quali risiedono i dati mission-critical della Società, sono conservati in locale separato a temperatura controllata con accesso riservato.

Vengono adottate funzionalità di fault-tolerance in modo da minimizzare il rischio che un guasto ad una delle componenti del sistema informatico provochi l'interruzione dell'operatività della Società e/o la corruzione o la perdita di dati. Per i dati mission-critical la soluzione adottata è quella della moltiplicazione delle componenti server, grazie ad un cluster hardware che combina più server con ridondanza di processori, memoria RAM, dischi e alimentatori.

Vengono adottate diverse procedure di backup: una prevede la preparazione giornaliera di una copia fisica su nastro di tutti gli archivi relativi di dati mission-critical (in particolare, i database dei software gestionali) e di altri dati quali quelli relativi al file-system, alla Intranet; la cartuccia viene collocata in una cassetta di sicurezza bancaria; viene inoltre realizzato un backup incrementale settimanale di tutti i dati mission-critical, che viene conservato in modo permanente in una cassetta di sicurezza bancaria; parallelamente avvengono altri backup analoghi su NAS, per ovviare ad errori del backup su nastro; un'altra procedura prevede i backup di tutte le macchine virtuali su NAS, questo tipo di backup permette anche il ripristino rapido di un singolo file senza dover "ricostruire" la VM su cui risiede.

- tutti i server fisici della Società sono dotati di configurazione con dischi hot-swap in RAID che evita la perdita di dati in caso di guasto a un disco e consente la sostituzione a caldo dei componenti danneggiati, senza la necessità di spegnere le macchine;
- I file dei server virtuali e tutti i dati risiedono sulla SAN, dotata di doppio alimentatore, doppio controller in collegamento incrociato con i nodi ESX via switch in fibra (ridondati) e batteria di dischi fast sas a 15K in RAID 5 + 1 con hotspare per il general pourpouse, FLASHDISK in RAID5 con HotSpare per i db mission critical che necessitano di performance massime e 100 GB di FastChace Flash a disposizione per garantire massime performance a tutte quelle applicazione intensive-access.
- I server e la SAN sono coperti estensione di garanzia del produttore 24x7x4 che assicura l'intervento tecnico entro 4 ore dalla chiamata.
- La società è dotata di due potenti gruppo di continuità, un UPS da 20KVA attivo 24 h che stabilizza e filtra la corrente e garantendo energia in caso di mancanza di fornitura elettrica. Uno alimenta la

sala server l'altro il DRS e client degli utenti degli uffici operativi di Milano siti in via Camperio numero 8.

- Esiste una failover zone su sede remota nella quale risiedono in standby i serverfailover per il db server che si aggiornano in real time col server di produzione.
- Le macchine di produzione sono replicate nel disaster recovery site per garantire l'operatività della società in caso di inaccessibilità della sala server. Le repliche avvengono in modo asincrono ad orari stabiliti, con frequenze differenti in funzione della criticità e delle modifiche che avvengono sulla macchina replicata.

Processo di acquisizione delle firme

Nel processo di acquisizione, trasferimento e memorizzazione dei dati biometrici, all'interno di strutture dati denominate "vettori biometrici" intervengono diverse tecnologie di cifratura

STEP DEL SISTEMA DI CIFRATURA DEI DATI BIOMETRICI
La concatenazione di hash del documento e vettore biometrico viene cifrata con crittografia simmetrica standard con chiave AES a 256 bit e IV pre-condiviso tra client e server per la protezione dei dati
La chiave simmetrica viene a sua volta cifrata con algoritmo di crittografia a chiave pubblica RSA a 1024/2048 bit; la chiave privata è detenuta da un soggetto terzo fiduciario
I dati biometrici e la chiave simmetrica cifrata con chiave pubblica sono a loro volta incapsulati in una firma elettronica PDF formato PAdES, realizzata con un certificato di firma tecnica

La coppia di chiavi pubblica e privata sono generate da una CA con apposto atto.

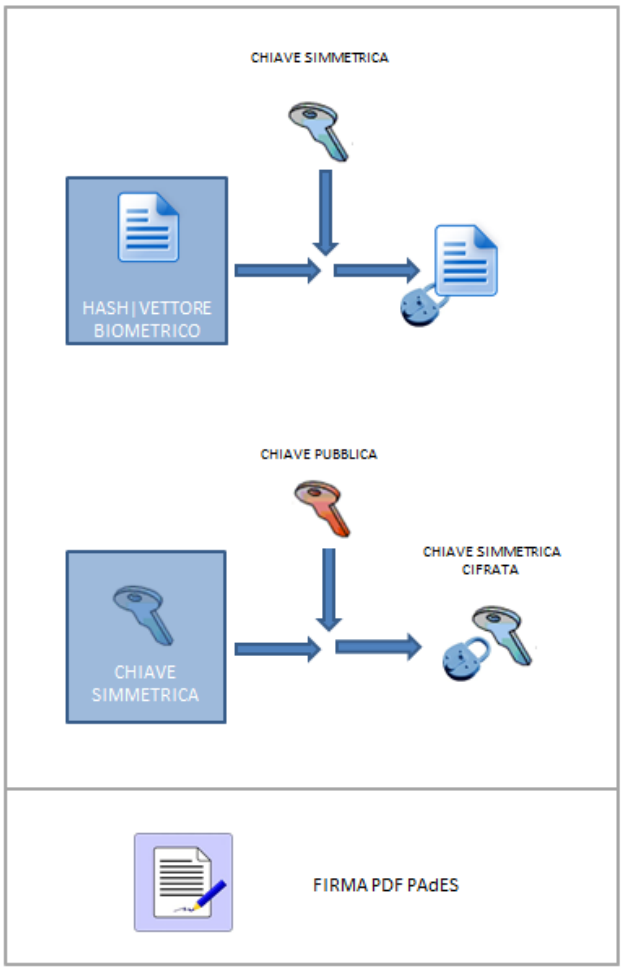
- La CHIAVE PUBBLICA DI CIFRATURA che è utilizzata dal Client di Firma per cifrare la chiave AES, che a sua volta è utilizzata per cifrare il vettore biometrici ed altre informazioni utili al processo di firma.

- La CHIAVE PRIVATA DI CIFRATURA, l'unica in grado di estrarre in chiaro la chiave AES, utilizzata per decifrare i dati biometrici, è conservata da un ente terzo fidato. La Terza Parte Fidata sarà chiamata dall'autorità giudiziaria in caso di contenzioso, e manterrà sempre il controllo sulla chiave, che non verrà mai messa a disposizione di CLIENTE

- Il CERTIFICATO ELETTRONICO, – chiamato "Certificato di Firma tecnica" – utilizzato per racchiudere i dati biometrici cifrati in firme PAdES nel documento, garantendone integrità ed immodificabilità.

Oltre alla protezione del dato biometrico è anche garantita l'immediata correlazione tra i dati biometrici (ottenuti facendo firmare l'utente sulla tavoletta) ed il documento.

La soluzione assicura una stretta correlazione tra dati biometrici e documento da firmare sulla tavoletta; il processo prevede di unire immediatamente l'impronta del documento (hash) ed i dati biometrici, direttamente nell'applicativo client, andando a realizzare quello che viene definito tecnicamente "document binding", una procedura in grado di dimostrare in maniera inequivocabile una correlazione fra documento e firma sul tavoletta.



La firma non è così memorizzata in modo generico ma legata nativamente al documento che l'utente avrà avuto modo di visionare pagina per pagina sul terminale.

Un altro importante aspetto è legato alla gestione delle chiavi di cifratura introdotte precedentemente. I dati biometrici e l'hash del documento su cui va apposta la firma saranno cifrati con chiave simmetrica. A sua volta la chiave simmetrica sarà cifrata con una chiave pubblica. La corrispondente chiave privata viene conservata in maniera sicura e custodita un soggetto terzo fiduciario.

La chiave privata potrà essere utilizzata in caso di contenzioso per dimostrare l'indissolubilità tra dati biometrici ed il documento. Solo così sarà sempre dimostrabile anche davanti ad un giudice sia il legame tra il sottoscrittore e lo specifico documento, che l'impossibilità per il titolare del processo di firma di accedere ai dati grafometrici raccolti o di collegare gli stessi ad altri documenti che non siano quelli volontariamente sottoscritti dal firmatario.

Sicurezza del vettore biometrico

Al momento dell'acquisizione di una firma il dispositivo di cattura (tavoletta esterna o superficie dello schermo + penna) trasferisce al software Unimatica i valori di diversi canali di campionamento.
Tipicamente si avranno i canali relativi a:

- Istante della rilevazione (T)
- Posizione orizzontale (X)
- Posizione verticale (Y)
- Presenza di contatto tra la penna e la superficie (S)
- Forza esercitata dalla penna sulla superficie (F)

Questi dati costituiscono il "vettore biometrico" della firma e sono l'oggetto principale di cui viene richiesta la protezione dalle regolamentazioni in materia di garanzie sulla privacy. Essi possono permettere di verificare, in sede di perizia, l'identità del firmatario.

Per la realizzazione della corrispondente firma elettronica sul documento è inoltre necessario costruire un legame univoco e indissolubile tra il vettore biometrico ed il contenuto digitale che è oggetto della sottoscrizione. Questo collegamento è garantito dalla compresenza dell'impronta del contenuto (hash) e del vettore biometrico nello stesso oggetto informatico che costituirà l'evidenza della sottoscrizione.

Questo oggetto viene protetto con tecnologie crittografiche in modo da renderlo decifrabile solo da un soggetto terzo fiduciario - nel caso specifico di Consultinvest Investimenti SIM SpA , rappresentato da un Notaio della Repubblica Italiana - che ha l'incarico di generare la coppia di chiavi asimmetriche (pubblica e privata) e di conservare e utilizzare in modo esclusivo la sola chiave privata.
Il software di acquisizione non persiste mai in memoria il dato biometrico in chiaro (non protetto).
Per queste ragioni un'eventuale compromissione del dispositivo in uso o delle trasmissioni non permetterebbe di ottenere i dati biometrici, ma soltanto una versione finale e già protetta con il massimo delle misure crittografiche del vettore.
Per ragioni di efficienza, e com'è prassi comune e standardizzata, la cifratura del vettore biometrico viene eseguita in due passi.
Si usa un algoritmo simmetrico più efficiente per la cifratura dei dati. In questo passaggio la chiave della cifratura simmetrica ha una parte generata ogni volta casualmente al momento della protezione.
La parte casuale della chiave viene poi cifrata con l'algoritmo a chiavi asimmetriche, facendo uso della chiave pubblica associata a quella privata e custodita dal soggetto terzo fiduciario.
In fase di decifratura si potrà usare la chiave privata per ottenere la chiave simmetrica casuale e poi usare la chiave simmetrica per avere il vettore biometrico in chiaro.
In questo momento sarà anche disponibile l'impronta del contenuto firmato che sarà usata per verificare l'integrità del documento sottoscritto.

Protezione del dato biometrico sul dispositivo

Come visto precedentemente, per la creazione del "vettore biometrico cifrato" nella sua forma finale è necessario disporre dell'impronta del contenuto digitale oggetto della sottoscrizione. Questo porta a dover distinguere due casi di funzionamento nei dispositivi in mobilità:

- Firme eseguite in presenza di connettività (on-line)
- Firme eseguite in assenza di connettività (off-line), modalità non prevista da Consultinvest Investimenti SIM SpA

La principale differenza dei due scenari è costituita dalla possibilità di calcolare ad ogni firma l'impronta della nuova "revisione" del documento PDF.

Le firme PADES vengono gestite come una "matrioska" di firme successive in cui ogni firma crea una nuova revisione del documento PDF, che sarà a sua volta il contenuto firmato al passo successivo.

Nello scenario on-line l'applicazione di raccolta della firma, ad ogni firma acquisita, utilizza l'impronta della revisione precedente per costruire immediatamente il vettore cifrato che poi trasmette agli appositi servizi web esposti dal server UNISERV (protetti con tecnologia SSL).

Ad ogni chiamata il server compone la nuova revisione del documento PDF e restituisce all'applicazione l'impronta corrispondente, che sarà nuovamente usata per la prossima firma.

Nello scenario off-line, escluso da Consultinvest Investimenti SIM SpA, non è invece possibile effettuare questo dialogo con il server, per definizione, e quindi l'applicazione, che per motivi di efficienza e di sicurezza non gestisce localmente i PDF, non è in grado di comporre la successiva revisione ed avere l'impronta.

In questo caso il vettore biometrico viene comunque cifrato subito con la chiave pubblica del soggetto terzo fiduciario, ma l'impronta viene sostituita con un'impronta legata al contenuto del documento base, costante e non progressiva per la successione di firme.

Quando saranno ripristinate le condizioni di connettività, le firme off-line verranno sincronizzate col server ed i vettori corrispondenti saranno utilizzati per comporre un nuovo oggetto informatico, analogo al vettore cifrato, in cui anziché avere il vettore in chiaro verrà incluso il vettore già cifrato e l'impronta della revisione corrente.

E' evidente che in fase di decifratura si dovrà semplicemente utilizzare l'algoritmo due volte con la stessa chiave privata per ottenere i dati in chiaro. L'impronta da usare per la verifica di integrità del documento è quella ottenuta al primo passaggio. L'altra potrà essere trascurata, essendo necessaria solo per i controlli eseguiti dal server UNISERV in fase di costruzione del documento PDF.

Strutture dati per la protezione dei dati grafometrici

Vengono di seguito descritte le specifiche tecniche delle strutture dati utilizzate per la protezione dei dati grafometrici.

Struttura del vettore biometrico

Il vettore biometrico è in formato XML. La struttura è la seguente:

```
<?xml version='1.0' encoding='UTF-8' standalone='yes' ?>
<SignatureData>
  <Points>
    <PenPoint>
     <X>int</X>
     <Y>int</Y>
     <Pressure>float</Pressure>
     <Time>uint</Time>
    </PenPoint>
    [...]
  </Points>
</SignatureData>
```

dove:

- le coordinate sono interi;
- la pressione è relativa, quindi float ∈ [0, 1];
- il tempo (in millisecondi) è relativo, quindi naturale ∈ [0, ∞), dove il primo campione deve aver valore 0.

Eventuali dati raw sono esclusi dal vettore biometrico in quanto non necessari.

Esempio:

```
<?xml version='1.0' encoding='UTF-8' standalone='yes' ?>
<SignatureData>
  <Points>
    <PenPoint>
       <X>58</X>
       <Y>395</Y>
       <Pressure>0.222321145</Pressure>
       <Time>0</Time>
    </PenPoint>
    <PenPoint>
       <X>60</X>
       <Y>400</Y>
       <Pressure>0.288998907</Pressure>
       <Time>5</Time>
    </PenPoint>
    [...]
  </Points>
</SignatureData>
```

Struttura del dizionario di firma pdf

La struttura del dizionario di firma PDF è stata costituita sulla falsa riga di **Digital Signature Build Dictionary Specification**, February 29, 2008 (), aggiungendo eventualmente ulteriori campi.

Tale struttura è costituita principalmente da due gruppi di oggetti:

- uno che definisce i dati biometrici e il dispositivo fisico con cui sono stati raccolti;
- l'altro che descrive gli applicativi client e server tramite i quali è stato prodotto il documento firmato;

Inoltre è presente un ulteriore campo il cui contenuto è modellato a seconda delle esigenze del cliente: /Prop_AdditionalInformation.

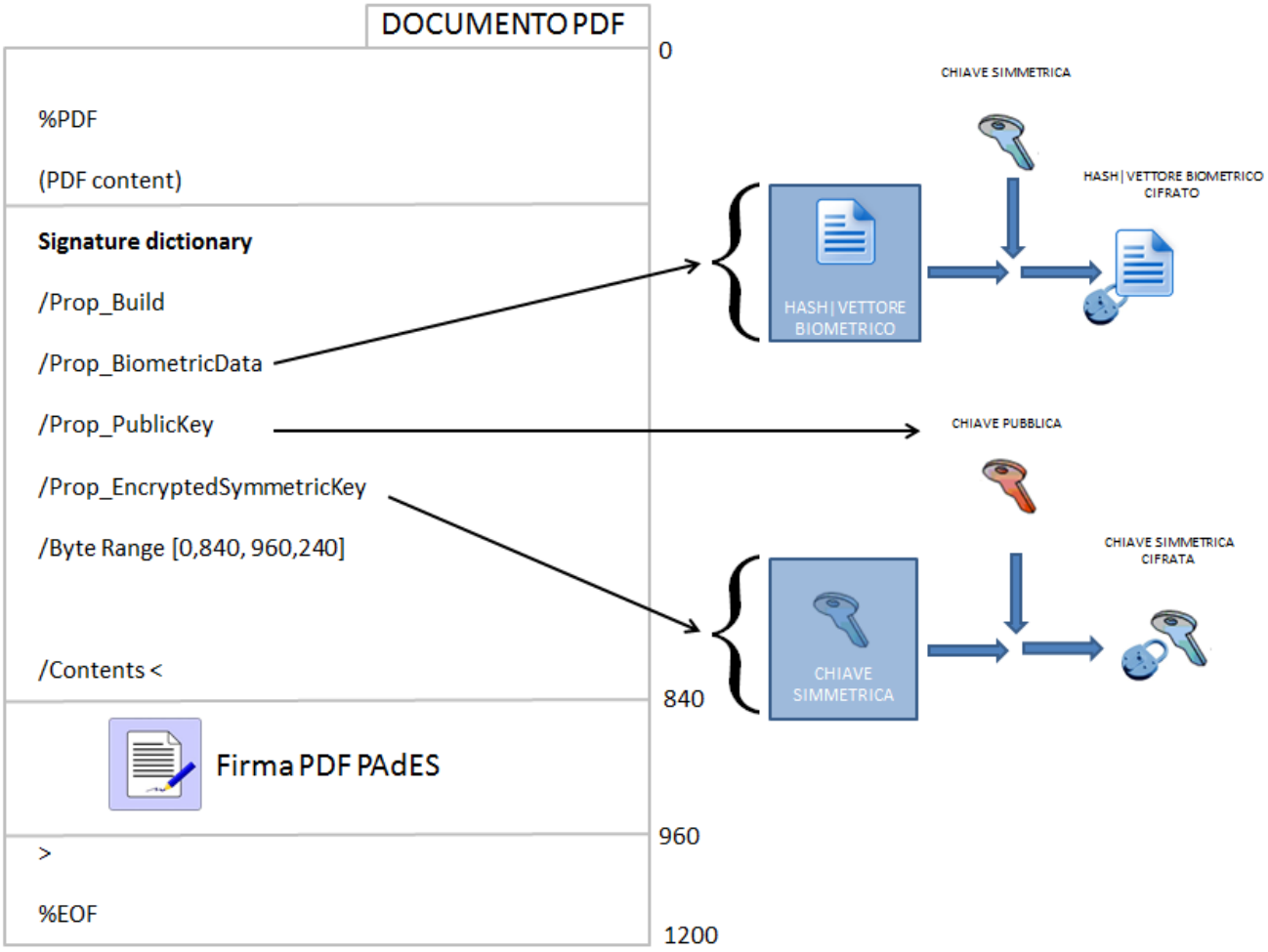
Al primo gruppo appartengono:

Nome	**Descrizione**
/Prop_BiometricData	Concatenazione dell'hash del documento aggiornato all'ultima revisione e del vettore biometrico cifrata con la chiave simmetrica e convertita nel formato Base64.
/Prop_EncryptedSymmetricKey	Chiave simmetrica cifrata con la chiave pubblica e convertita nel formato Base64.
/Prop_PublicKey	Chiave pubblica utilizzata per la cifratura della chiave simmetrica, rappresentata nel formato RsaKeyValue e convertita nel formato Base64.
/Prop_Device	Oggetto avente come figli /Name e /SerialNumber.
/Name	Nome descrittivo del dispositivo tramite il quale è stata ottenuta la firma.
/SerialNumber	Identificativo univoco del dispositivo con cui è stata apposta la firma.

Il secondo gruppo di campi è costituito da:

/Prop_Build	Campo contenente /Filter, /PubSec e /App.
/Filter	Campo contenente /Name, /Date, /R e /PreRelease. Descrive l'applicativo che gestisce l'aggiunta delle firme PDF.
/Name	Nome di tale applicativo.
/Date	Data di build di tale applicativo.
/R	Versione di tale applicativo.
/PreRelease	Da impostare a "false", indica che la firma è stata generata da un

	software rilasciato e non di test.
/PubSec	Campo contenente /Date, /R, /PreRelease e /NonEFontNoWarn. Come /Filter, descrive il modulo software che gestisce l'aggiunta delle firme al PDF.
/Date	Data di build di tale applicativo.
/R	Versione di tale applicativo.
/PreRelease	Da impostare a "false", indica che la firma è stata generata da un software rilasciato e non di test.
/NonEFontNoWarn	Da impostare a "true" per indicare all'applicazione che visualizza il PDF (e.g. Adobe Reader) di non mostrare un warning nel caso in cui non sia stato effettuato l'embedding dei font.
/App	Campo contenente /Name, /REX, /R, /Date, /OS e /OsCapturingDevice. Descrive l'applicativo che gestisce il processo di firma.
/Name	Nome di tale applicativo.
/REx	Versione di tale applicativo.
/R	Versione di build di tale applicativo.
/Date	Data di rilascio di tale applicativo.
/OS	Lista dei sistemi operativi su cui può essere eseguito l'applicativo che produce il PDF aggiungendo le firme.
/OSCapturingDevice	Sistema operativo su cui viene eseguito l'applicativo che cattura la firma.



Esempio di dizionario di firma nel caso di utilizzo di UniservPen nella modalità online che prevede la comunicazione con Uniserv per tutta la durata del processo

```
/Prop_BiometricData                [Base64 applicato al risultato della cifratura della concatenazione dell'hash del documento alla revisione corrente e del vettore biometrico]
/Prop_EncryptedSymmetricKey        [Base64 applicato al risultato della cifratura della chiave simmetrica]
/Prop_Device
  /Name                            DTU-1031
  /SerialNumber                    3CZQ000813

/Prop_AdditionalInformation

/Prop_Build
  /Filter
    /Name                          /Unilet-Biometrica
    /Date                          2013-11-30T10:12:22CET
    /R                             000500030054
    /PreRelease                    false

  /PubSec
    /Date                          2013-11-30T10:12:22CET
    /R                             000500030054
```

```
  /PreRelease               false
  /NonEFontNoWarn           true

/App
  /Name                     /Uniserv
  /REx                      1.11.4
  /R                        123
  /Date                     2013-12-17T15:12:22CET
  /OS                       [Linux]
  /OSCapturingDevice        Windows 8
```

Estrazione dei dati grafometrici e verifica delle firme

Il processo di crittografia dei dati biometrici, come descritto nel precedente paragrafo, si avvale di un certificato di crittografia basato su due chiavi asimmetriche, una pubblica ed una privata, basate sullo standard RSA. Nel processo attuato le due chiavi asimmetriche sono generate da un soggetto terzo fiduciario che provvede inoltre alla custodia e conservazione "notarile" della chiave privata, oltre che alla consegna della chiave pubblica che è utilizzata da Uniserv per crittografare i vettori biometrici della firma grafometrica.

La chiave privata viene conservata dal "Terzo Fidato" in modo sicuro e garantito nel tempo, tramite il Notariato, che consente anche il passaggio in successione di questo elemento (chiave privata necessaria per l'apertura dei vettori biometrici) nel caso di impedimento o scomparsa dello stesso Notaio.

Il processo del soggetto terzo fiduciario comprende anche la procedura adottata per rendere disponibile, in sua presenza e sotto la sua responsabilità, la chiave privata, indispensabile per l'apertura del "vettore biometrico" in caso di contestazione e/o contenzioso e perizia calligrafica.

Consultinvest Investimenti SIM SpA ha deciso di incaricare il Notaio Eugenio STUCCHI a ricoprire il ruolo di Soggetto Terzo Fiduciario ai fini della generazione e conservazione delle chiavi di asimmetriche.

Lo stesso Notaio ha provveduto, tramite apposito Atto, a descrivere la procedura adottata.

Procedura di verifica e perizia calligrafica

In caso di eventuale contenzioso vengono sottoposti al Notaio i dati biometrici criptati, che vengono decodificati a mezzo della chiave privata conservata. Il processo di decodifica avviene in modalità sicura, con i medesimi standard sopra descritti per il processo di generazione.

Replicando quanto avviene nel mondo cartaceo in caso di esame delle sottoscrizioni delle parti effettuato dai periti, l'esame del dato biometrico avviene nello studio notarile, presso una postazione dedicata, sotto il controllo continuo del Notaio, che redige di tale processo idonea certificazione in atto pubblico.

Dato qualificante, anch'esso riconducibile all'intervento del Pubblico Ufficiale, è che durante tutto tale processo la chiave privata viene mantenuta segreta per non invalidare eventuali altri documenti con la stessa firmati.

A fronte di una richiesta di perizia, è previsto il seguente scenario:

1. Il documento oggetto di perizia viene consegnato al soggetto terzo fiduciario che ha il possesso esclusivo della chiave privata corrispondente alla chiave pubblica con cui i vettori sono sigillati nel documento digitale.
2. Per mezzo di un apposito software il soggetto terzo fiduciario esegue l'apertura del vettore biometrico cifrato ed estrae il vettore biometrico in chiaro e l'impronta del contenuto originale firmato.
3. Successivamente il soggetto terzo fiduciario verifica l'integrità del contenuto del documento ricalcolandone l'impronta che deve risultare identica a quella sigillata nel vettore biometrico cifrato.
4. Il soggetto terzo fiduciario certifica l'avvenuta verifica dell'integrità e di estrazione del vettore biometrico in chiaro.

5. Il soggetto terzo fiduciario rende disponibile il vettore biometrico in chiaro ai periti nominati dall'autorità giudiziaria.

Il vettore biometrico in chiaro è una rappresentazione informatica in formato non proprietario che quindi può essere visualizzato anche con altri strumenti. Unimatica propone un proprio tool, denominato Calligraphy (nella figura sottostante).

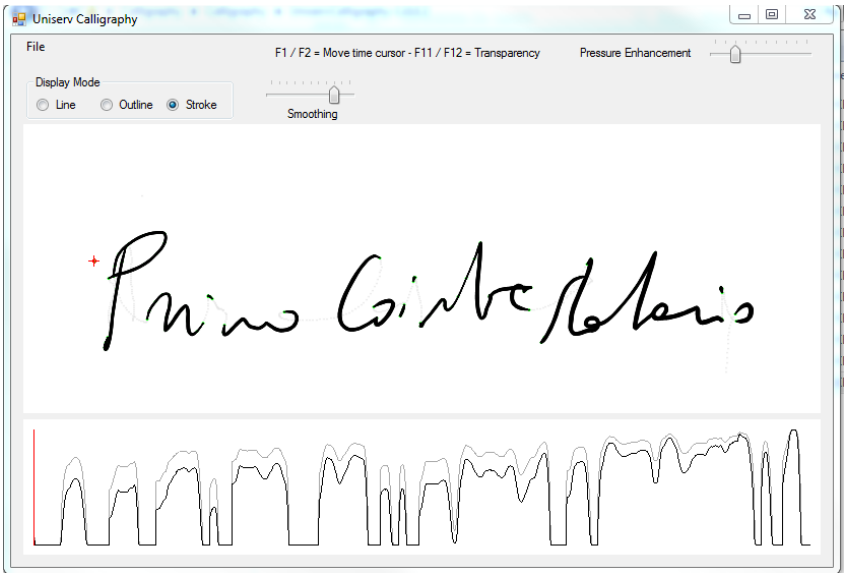


Figura 1

Le principali caratteristiche di Uniserv-Calligraphy sono le seguenti:

1. Display della firma in modalità "campioni"
2. Display della firma in modalità "outline" o "stroke", con una rappresentazione grafica del dato pressorio in forma di inspessimento del segno (in analogia con la firma cartacea)
3. Rappresentazione dei campioni "in volo"
4. Display sincronizzato del dato di pressione
5. Funzioni di ingrandimento e posizionamento ("zoom e pan") sul display bidimensionale della firma
6. Animazione del cursore che può muoversi nella sequenza dei campioni sotto il controllo dei tasti funzione (modalità "jog")
7. Funzione per il controllo della tensione della line di raccordo usata nell'interpolazione tra i campioni ("smoothing")
8. Funzione di "esaltazione" della pressione ("Enhancement") per massimizzare la rappresentazione anche a fronte di valori pressori scarsamente distribuiti
9. Controllo della trasparenza della Window per consentire sovrapposizioni in trasparenza, sia con altri campioni grafometrici che con immagini derivanti da scansione di campioni autografi cartacei.

Va da sé che tale perizia può essere effettuata con il consenso delle parti in causa, assistiti dai propri legali ed eventualmente dai periti di parte.

Caratteristiche della generazione dei certificati di cifra

Generazione a mezzo della CA del Notariato

Il Notaio (*Soggetto Terzo – Notaio incaricato*), su incarico di Consultinvest Investimenti SIM SpA, procede alla generazione della coppia di chiavi asimmetriche (pubblica e privata). La procedura prevede la generazione remota delle chiavi di cifra in forma di certificato X-509, da parte della Certification Authority di Servizio del Notariato, cosiddetta CA, accreditata presso l'Agenzia per l'Italia Digitale "AgID". Affinché sia garantita la riservatezza della chiave di privata, il Notaio incaricato procede alla generazione della coppia di chiavi in una data concordata con il responsabile tecnico incaricato da Consultinvest Investimenti SIM SpA.

Con questa procedura il Notaio agendo quale L.R.A. (Local Registration Authority) della CA in modalità sicura identificato a mezzo token di firma univoci provvede a generare i certificati di cifra su HSM specificamente dedicati a tale procedura, gestiti direttamente dal Notariato italiano. La parte privata del certificato non viene mai in possesso del Notaio e rimane residente sui sistemi centralizzati del Notariato.

In caso di eventuale decodifica, sempre a mezzo di autenticazione remota, il dato biometrico criptato viene sottoposto telematicamente all'HSM il quale restituisce il dato in chiaro in modo da poter essere così esaminato.

All'atto della generazione delle chiavi il Notaio stila un corrispondente atto che include esplicitamente il riferimento a Consultinvest Investimenti SIM SpA come destinatario dei servizi relativi.

Consegna e conservazione della chiave privata

Nel processo attuato da Consultinvest Investimenti SIM SpA, il soggetto terzo fiduciario coincide con quello incaricato per la generazione della chiave privata e quello delegato alla sua custodia e conservazione.

La coppia di chiavi asimmetriche per la cui generazione Consultinvest Investimenti SIM SpA ha incaricato il soggetto terzo fiduciario, è di piena ed esclusiva titolarità giuridica di Consultinvest Investimenti SIM SpA medesimo che, pertanto, risulta essere soggetto responsabile della sua conservazione. Il Notaio incaricato, soggetto terzo fiduciario, delegato da Consultinvest Investimenti SIM SpA alla custodia e conservazione della chiave privata, agisce in forza di un mandato professionale senza rappresentanza.

Durata dei certificati e generazione nuove chiavi

I certificati di cifra hanno durata triennale, la quale tuttavia trattandosi di certificati di cifra e non di firma non ha alcuna ripercussione giuridica sulla validità dei documenti con essi cifrati, ma serve unicamente come parametro di organizzazione interna e di processo. L'unica vera "durata" del certificato di cifra è data dalla sua obsolescenza tecnologica, la quale tuttavia è incerta, ma ampiamente sorpassata dall'utilizzo di chiavi di lunghezza adeguata e ridondante.

Consultinvest Investimenti SIM SpA ha predisposto una procedura da mettere in atto nell'eventualità in cui sia necessaria, la generazione delle nuove chiavi, che coinvolge il fornitore che ha realizzato la soluzione di firma e la Terza Parte Fidata.

- Consultinvest Investimenti SIM SpA darà ordine di procedere con la generazione e attivazione di una nuova coppia di chiavi asimmetriche (chiave pubblica e privata).

- Entro due settimane [durata stimata di quanto in media trascorre tra la richiesta e l'emissione del certificato] dall'ordine il Notaio provvede alla generazione delle chiavi, con la procedura precedentemente descritto.
- Successivamente alla generazione della chiave è previsto che un documento di test venga sottoposto alla Terza Parte Fidata al fine di verificare la corretta estraibilità dei vettori biometrici
- In coordinamento con Unimatica, una volta eseguite le verifiche necessarie, la nuova chiave viene attivata sui sistemi di produzione in data e con modalità concordate con i tecnici di Consultinvest Investimenti SIM SpA.

Continuità operativa

Consultinvest Investimenti SIM SpA ha deciso di appoggiarsi alla struttura della CA del Notariato italiano. Questo consente di dare al servizio un'altissima continuità operativa in quanto la parte privata del certificato risiede non solo su HSM di una CA accreditata, ma su HSM di una CA appartenente ad un "ente pubblico" quale è appunto il Consiglio Nazionale del Notariato, con conseguenti assolute garanzie di continuità.

In caso di cessazione dal servizio del notaio incaricato della generazione i codici di accesso agli OTP che fungono da autenticazione possono essere trasferiti manualmente a qualsiasi altro notaio italiano specializzato in tali servizi, che pertanto potrà così procedere a tutte le operazioni previste dal processo di firma grafometrica, tra cui gli audit periodici, le verifiche, e le nuove generazioni.

Cenni professionali del Notaio incaricato

Il Notaio Eugenio Stucchi è membro della Commissione Informatica del Consiglio Nazionale del Notariato, e si occupa specificamente dell'implementazione della cosiddetta "fase due" del Servizio di Conservazione a Norma del Notariato italiano, SCNN con l'apertura dello stesso a processi di key-escrow e blind-escrow, e più in generale a tutto quanto non costituisce strettamente atto pubblico notarile.

È altresì membro del gruppo ristretto che segue l'implementazione della CA di Servizio del Notariato italiano e delle relative funzioni.

È socio fondatore e direttore del Comitato Scientifico dell'Associazione Italiana Firma Elettronica Avanzata biometrica e Grafometrica, A.I.F.A.G. (www.aifag.it), ed è intervenuto in numerosi convegni ed incontri sul tema della firma grafometrica.

Ha quindi collaborato in diversi progetti di implementazione di firma elettronica avanzata a mezzo firma grafometrica in collaborazione con alcune tra le maggiori aziende software di settore italiane, per conto di diversi clienti tra cui istituti bancari, assicurativi, aziende di lavoro interinale, aziende nel campo retail e biomedicale.

Recapiti

Notaio Eugenio STUCCHI
Via dei Mercanti, 2 - 10122 TORINO
tel. 011 5176094
eugenio.stucchi@notariato.it
eugenio.stucchi@postacertificata.notariato.it

Processo di conservazione digitale dei documenti

I documenti digitali prodotti dal processo di firma vengono conservati utilizzando il sistema di conservazione UNISTORAGE di Unimatica (che è conservatore accreditato).

I servizi di conservazione digitale sono regolamentati dallo specifico Manuale di Conservazione. La versione standard del Manuale del Servizio di Conservazione è inoltre scaricabile direttamente dal portale internet dell'AgID nella sezione "Elenco dei certificatori Accreditati".

In particolare per i documenti con firma grafometrica lo stesso sistema di generazione UNISERV provvede alla creazione di una copia priva dei vettori grafometrici (cosiddetta copia "PDF flat"). Questa copia PDF flat sarà quella utilizzata per tutti gli scopi correnti, quali invio di copie al Cliente e/o memorizzazione sui sistemi gestionali e documentali.

La copia originale, contenente i vettori grafometrici sarà custodita solo nel sistema di conservazione e prodotta su richiesta della SIM. Ad esempio in caso di verifica presso il soggetto terzo fiduciario.

Come documentato nel Manuale della Conservazione, il documento sarà reso disponibile con il corredo delle evidenze di conservazione, che attestano in modo pubblicamente verificabile l'integrità e l'autenticità dell'oggetto digitale conservato.

Il sistema di conservazione UNISTORAGE, essendo nativamente integrato con il processo di gestione della firma grafometrica è in grado di produrre anche successivamente copie PDF flat dei documenti conservati.