Strumenti tecnologici utilizzati

La firma elettronica avanzata in modalità grafometrica si ottiene dal rilevamento dinamico dei dati calligrafici della firma effettuata con penna elettronica.
Il processo prevede l'apposizione della firma autografa del cliente su un apposito tablet, che rileva le informazioni di biometria comportamentale tipicamente inferite da un perito calligrafo, e utilizzate per imputare una firma a un soggetto. Per elaborare queste informazioni (blob biometrico) sono utilizzati specifici device (tavolette di firma – Tablet) e software ad hoc per pilotare i device e acquisire i dati di biometria comportamentale.

L'utilizzo congiunto di questi device HW, dello specifico SW e delle soluzioni di certificazione consente di rendere autoconsistente, il documento, che contiene i dati biometrici cifrati.

Di seguito vengono riportate le principali componenti tecnologiche utilizzate nella soluzione

Tablet

I device utilizzati per l'apposizione della firma grafometrica sono dispositivi HW in grado di rilevare i principali parametri (posizione, tempo , pressione, velocità, accelerazione) della firma dell'utente.

I parametri che caratterizzano il funzionamento dei tablet tipicamente sono:
• la frequenza di campionamento
• la risoluzione in acquisizione
• l'intervallo di acquisizione – Asse X
• l'intervallo di acquisizione – Asse Y
• livelli di acquisizione della pressione
• l'area attiva
• la dimensione del display LCD
• la risoluzione del display LCD
• la dimensione del pixel

Nello specifico SEC Servizi, a seguito di un attività di software e hardware selection ha deciso di adottare il tablet ENsign 10 di Euronovate di cui riportiamo di seguito le caratteristiche tecniche fornite dal produttore.

• Specifiche Generali:
- Display a colori da 10,1 pollici
- "USB to VGA" per Microsoft Windows XP/VISTA/7©
- Dimensioni ~263x173x16 mm
- Peso ~750gr
• Schermo
- Pannello 16:9 LCD 10.1 pollici TFT
- Risoluzione Video 1024 x 600
- 262K colori
- Retroilluminazione LED
- Protezione con video temperato
• Caratteristiche di firma
- Tecnologia Elettromagnetica
- Penna senza batteria
- Risoluzione di 1000 LPI
- Area attiva 222 x 125 mm
- 1024 livelli di pressione (10bit)
- Forza applicabile : 30g – 500g
- 150 campioni al secondo
- Rilievo dei movimenti aerei fino a 10mm

• Sicurezza Software e Hardware
- Case monoscocca, sigillato senza viti
- Cavo USB non staccabile dal tablet
- Crittografia standard 3DES durante la comunicazione

Il Display a colori da 10.1 pollici di ENsign10 consente la rappresentazione dell'intero documento sul tablet. Tramite l'utilizzo della penna elettronica è possibile effettuare lo scroll e lo zoom del documento e apporre la propria firma negli appositi campi firma. Completata la firma l'utente può decidere di accettarla premendo con la penna un pulsante di OK sulla tavoletta o di rifarla annullando l'operazione appena compiuta.

E' inoltre presente una barra strumenti che consente
- zoom
- pagina successiva
- pagina precedente
- inizio documento
- fine Documento

La stessa barra strumenti prevede inoltre la possibilità di passare alla firma successiva (o precedente), saltando la visualizzazione delle singole clausole o pagine del documento.

Software di pilotaggio

Il software selezionato da SEC Servizi per pilotare il tablet ENsign10 e per l'acquisizione e l'incapsulamento dei dati biometrici all'interno del documento è ENSoft di Euronovate.

Secondo quanto dichiarato dal fornitore:

"L'architettura del SW, per esigenze di adattamento alle diverse situazioni presenti sul mercato, è stata sviluppata a moduli che si basano sulle seguenti considerazioni generali.
• L'applicazione di firma deve essere locale alla workstation cui è collegato il tablet.
• L'ambiente locale può essere un ambiente "fisico" (PC) oppure remotizzato con soluzioni di mercato (Citrix/ XenDesktop). In quest'ultimo caso la macchina cui è colegato il tablet potrebbe essere anche uno Zero-Client"…

…"ENSoft racchiude al suo interno 3 differenti macro-moduli.
*1. **ENTablet** : Driver di basso livello che tramite le librerie del digitlizzatore, espone una serie di metodi per un integrazione di base legata all'acquisizione dei vettori biometrici.*
*2. **Document Manager** : Oggetti per la manipolazione del documento PDF.*
• Scansione del documento per l'individuazione dei campi firma.
• Modifica dei campi firma individuati per la creazione degli e-signature all'interno dello stesso documento PDF
*3. **ENSigner** : Modulo per la cattura della firma sul Tablet e successivo inserimento del blocco all'interno del PDF" …*

"Come vengono inseriti i dati biometrici all'interno del PDF
Una volta ottenuto il vettore biometrico (quindi subito dopo aver acquisito i dato della firma del cliente), questo viene legato in modo indissolubile al documento a cui fa riferimento.
Viene quindi calcolato l'HASH del documento PDF prima dell'esevuzione della firma.
L'Hash del documento e il vettore biometrico della firma, vengono incapsulati all'interno di un unico oggetto definito "Blocco Biometrico" e vengono cifrati con una chiave simmetrica blowfish128 generata al volo al momento della firma.
La chiave simmetrica utilizzata per la cifratura del vettore biometrico, viene a sua volta cifrata con la chiave pubblica e viene inserita come "header" del blocco biometrico precedentemente creato.

Viene poi aggiunto a tutto, un secondo header in chiaro contenente alcuni elementi per il riconoscimento della versione dell'oggetto utilizzato per il trattamento del blocco biometrico.
L'intero pacchetto (Blocco biometrico, Header Cifrato e Header in chiaro) viene poi convertito in ASCII ed inserito in una nuova voce del dizionario del campo firma creata ad-hoc per il contenimento dei dati.
Il Campo firma viene quindi utilizzato per firmare digitalmente il documento con una firma di integrità che ne garantisce l'immodificabilità e viene inserita nel punto firma l'immagine della firma del cliente."

Strumenti di cifratura

Per garantire un adeguato livello di sicurezza del processo di firma grafometrica è fondamentale che i dati biometrici vengano cifrati con chiave asimmetrica (pubblica) e incapsulati all'interno del documento.
Per la cifratura del blob biometrico e l'eventuale decifratura per le verifiche legali durante un contenzioso, la soluzione utilizzerà una coppia di chiavi RSA (2048 bit) fornite dalla **Certification Authority** di riferimento la cui chiave pubblica si utilizza in fase di cifratura dei dati e la parte privata invece diventa necessaria per la parte di decifratura.
Le chiavi (RSA di 2048 bits) sono prodotte in ambiente protetto (su computer all'interno dei locali CA), alla presenza del funzionario della sicurezza e dell'amministratore dei sistemi di CA. Il Software utilizzato è OPENSSL. Le chiavi create sono cifrate con algoritmo aes256 e la PWD di protezione è di 16 caratteri alfanumerici. A partire dalla chiave sono generati il certificato e il PKCS #12.
Il PKCS #12 è cifrato con algoritmo AES256 e la password di protezione è di 16 caratteri. La chiave privata e il certificato sono caricati su 5 dispositivi sicuri[4], il PKCS#12 su 2 CD e il certificato su un CD.
Dopo tali operazioni le chiavi, il certificato ed il PKCS #12 sono cancellati con metodo NSA a 7 passaggi.
Al termine è redatto un verbale, firmato dai presenti e conservato nel sistema di conservazione.

La chiave privata così creata potrà essere conservata direttamente dalla CA o da una altra terza parte fidata, secondo una procedura sicura, che prevede che i dispositivi sicuri e i CD che contengono le chiavi (i CD conterranno anche le librerie per l'utilizzo delle chiavi) siano inseriti in 6 buste sigillate. Ad ogni busta (esclusa quella contenente il certificato da consegnare al destinatario) corrisponde un'altra busta sigillata contenente il PIN/PUK5 del dispositivo o la password del PKCS #12.
Le buste sigillate sono così 12 con le seguenti caratteristiche:

- busta contenente un dispositivo sicuro e relativa busta contenente PIN/PUK. Utilizzata per la verifica dei Blob cifrati e conservata all'interno della cassaforte del bunker CA o di un eventuale altra terza parte fidata.
- busta contenente 1 CD con certificato da consegnare al destinatario. Al momento della consegna, effettuata dal funzionario della sicurezza della CA, verrà redatto un verbale
- busta contenente 2 dispositivi sicuri e relativa busta contenente PIN/PUK. Utilizzata come copia di riserva e conservata all'interno della cassaforte del bunker CA o di un eventuale altra terza parte fidata.
- busta contenente 1 CD e relativa busta contenente PWD. Utilizzata come copia di riserva e conservata all'interno della cassaforte del bunker CA o di un eventuale altra terza parte fidata..
- busta contenente 2 dispositivi sicuri e relativa busta contenente PIN/PUK. Utilizzata come copia di riserva e conservata all'interno della cassaforte del sito di Disaster Recovery della CA o di un eventuale altra terza parte fidata.
- busta contenente 1 CD e relativa busta contenente PWD. Utilizzata come copia di riserva e conservata all'interno della cassaforte del sito di Disaster Recovery della CA o di un eventuale altra terza parte fidata.

Annualmente il responsabile dell'audit della CA procede a controllare l'integrità delle buste e verifica la funzionalità dei dispostivi sicuri e dei CD che ospitano il PKCS #12, redigendo un verbale. Ogni due anni è eseguita una copia del CD, mentre l'originale è distrutto. Al termine il funzionario della sicurezza della CA, in presenza del responsabile dell'audit, inserisce i dispositivi sicuri, i relativi PIN/PUK, i CD e le relative password all'interno di nuove buste che sono sigillate, con apposizione della data.

4 Il dispositivo sicuro è un dispositivo crittografico rispondente a requisiti di sicurezza determinati da opportune

certificazioni di sicurezza. Può essere una smart card, un token USB, un HSM.
5 PIN Personal Information Number: codice identificativo associato ad un dispositivo sicuro / PUK Personal Unblocking Key: codice personalizzato utilizzato per riattivare il PIN del proprio dispositivo in seguito al blocco dello stesso per errata verifica del PIN stesso

Strumenti di certificazione

Al fine di garantire l'autoconsistenza del documento la banca utilizza strumenti di certificazione per l'apposizione di una firma d'integrità quali la firma automatica massiva e la successiva Conservazione a Norma del documento.

Firma Digitale Automatica Massiva

Il Servizio di Firma Automatica massiva, disponibile con tecnologia Web Services in modalità ASP consente di utilizzare Certificati di Firma Digitale senza che il titolare debba possedere alcun dispositivo crittografico (smart card o token USB).
Le chiavi (private e pubbliche) degli Utenti Titolari dei certificati sono generate e conservate presso la CA, su dispositivi sicuri ad alte prestazioni (Hardware Security Module o HSM).

Il Servizio consente al titolare ed all'applicazione da esso autorizzata di sottoscrivere digitalmente elevate quantità di documenti informatici secondo le normative vigenti utilizzando un Certificato Digitale che risiede su dispositivi sicuri presso la CA senza dover, per ogni documento, digitare le credenziali di autenticazione ed autorizzazione.
Il servizio è basato sulle regole tecniche emanate dalle competenti Autorità italiane. In particolare vengono recepite ed attuate le norme sancite:
• dal DPCM 29 marzo 2009
• delibera CNIPA n. 45/2009
• dal Codice dell'Amministrazione Digitale.

Il Servizio è formato da tre componenti integrate:
• un servizio automatico di firma digitale e marcatura temporale, ubicato presso la CA;
• un'applicazione già presente nel data center SEC Servizi che predispone i documenti informatici per l'apposizione della firma digitale e della marcatura temporale, gestendo l'invio e la ricezione degli stessi interfacciandosi con il servizio automatico presso la CA;
• un'applicazione che consente al Titolare, ovunque si trovi, di gestire in autonomia i certificati digitali per la firma automatica massiva.

Per legge, l'apposizione di firme digitali con procedura automatica, è valida se l'attivazione della procedura medesima è chiaramente riconducibile alla volontà del Titolare e lo stesso renda palese la sua adozione in relazione al singolo documento firmato automaticamente.
Questo significa che il Titolare del certificato di sottoscrizione per la firma automatica, deve avere la possibilità, in relazione ad una specifica applicazione di rendere "attiva" o "non attiva" la propria chiave privata (conservata dalla CA su HSM - Hardware Security Module).
Per tale motivo è stato definito un servizio Web, grazie al quale il Titolare, dopo essersi opportunamente autenticato, può attivare o disattivare la propria firma digitale.

Conservazione documenti

SEC Servizi ha da tempo scelto il Servizio di Conservazione sostitutiva dei documenti LegalDoc di InfoCert, disponibile in modalità ASP, che permette di mantenere e garantire nel tempo l'integrità dei documenti digitali, nel rispetto della normativa vigente.
In base a quanto stabilito dal quadro normativo di riferimento, le leggi e la normativa sulla conservazione sostitutiva dei documenti riconoscono piena validità legale alla conservazione in formato digitale dei documenti, purché le procedure adottate per la loro conservazione risultino conformi alle regole tecniche emanate.
Il servizio LegalDoc garantisce il pieno rispetto della normativa vigente in materia di conservazione

sostitutiva dei documenti ed è integrato con i sistemi SEC Servizi.
La Banca usufruendo affida ad InfoCert, in qualità di **Responsabile della Conservazione**, tutti gli oneri e le procedure di sicurezza, salvataggio, verifica periodica dei supporti, apposizione di firme digitali e marche temporali previsti dalla normativa di riferimento (in particolare l'art.5 della Deliberazione CNIPA n° 11/2004), per garantire il corretto svolgimento del processo di conservazione.