La soluzione di Firma Elettronica Avanzata (FEA) grafometrica

Le caratteristiche del sistema e le tecnologie utilizzate

novembre 2019

carifermo
cassa di risparmio di fermo s.p.a.

Indice

1. La Firma Elettronica Avanzata (FEA)

1.1. Che cosa è la FEA: ambito normativo

Fra le novità introdotte nel Codice dell'Amministrazione Digitale, così come modificato dal D.Lgs 235/2010, una delle più interessanti è certamente la previsione di un nuovo tipo di firma che può essere apposta con mezzi informatici: la firma elettronica avanzata. Il Legislatore, nel definirla, non ne precisa le caratteristiche tecniche, lasciando aperta la strada all'utilizzo di metodi diversi per apporre tale firma, partendo dall'impiego di codici di identificazione personali per arrivare a tecniche di tipo biometrico.

Una firma elettronica avanzata, in generale, potrà pertanto essere classificata a seconda del meccanismo di identificazione utilizzato:

- soluzioni basate sulla conoscenza, da parte del cliente utilizzatore, di un codice personale (something you know);
- soluzioni basate sul possesso, da parte del cliente, di un dispositivo assimilabile ad una carta (non necessariamente bancaria) o ad un token (something you have);
- soluzioni basate sull'utilizzo di un dispositivo in grado di rilevare alcune caratteristiche fisiche o comportamentali del cliente, come nel caso della firma grafometrica (something you are), che rientra nella definizione di firma elettronica avanzata.

La firma elettronica avanzata viene definita, nel C.A.D. (art. 1, comma 1°, lett. q-bis), come "un insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati".

Rientrano certamente fra questi mezzi, ad esempio, le "One Time Password" (OTP) basate su token fisici o le soluzioni di firma grafometrica realizzate con l'ausilio di specifici tablet.

Fra le possibili tipologie di firma elettronica avanzata, quella basata su tecniche grafometriche appare più sicura di quella basata su di un codice personale o token, i quali potrebbero essere utilizzati all'insaputa del legittimo possessore. Questo è uno dei motivi principali per cui è stata scelta in molti contesti, specialmente bancari.

I documenti informatici su cui sia stata apposta una firma elettronica avanzata hanno, inoltre, l'efficacia probatoria prevista dall'art. 2702 del Codice Civile per la scrittura privata e possono quindi essere utilizzati in molti scenari (fra cui in ambito bancario e/o assicurativo).

1.2. Come funziona la firma grafometrica

La firma grafometrica è un processo informatico che, nel rispetto di quanto previsto dal Codice dell'Amministrazione Digitale, implementa un particolare tipo di firma elettronica avanzata, in grado di sostituire una tradizionale firma autografa apposta su un documento cartaceo. Tale tipologia di firma si ottiene rilevando alcuni dati biometrici del firmatario, nel momento in cui egli appone la firma su di un tablet, legandoli in maniera indissolubile al documento oggetto di firma.

Per ottenere questo risultato, viene utilizzata una postazione di lavoro dotata di specifico software che interagisce con un tablet di firma. La stessa postazione permette al cliente (direttamente sul tablet) di visionare e scorrere il documento prima di firmarlo.

Eseguita la firma, questa può essere o meno confermata dal cliente; se infatti, quest'ultimo dovesse decidere, per qualunque motivo, di ripetere l'operazione, potrà farlo semplicemente annullando la firma apposta in precedenza.

Dal punto di vista del cliente non vi sono cambiamenti rilevanti rispetto a quanto accade in presenza di un documento cartaceo. Tuttavia, la Firma Grafometrica che si ottiene non è la semplice immagine di una firma, bensì qualcosa di più complesso, che tiene conto delle caratteristiche comportamentali (velocità, pressione, inclinazione, accelerazione e movimenti aerei) del cliente.

La soluzione tecnico-informatica approntata dal CSE, in collaborazione con IBM, prevede l'integrazione della Firma Grafometrica nell'applicativo di Sportello, al fine di dematerializzare le contabili delle operazioni, quindi, a tendere, l'intera busta di cassa.

La soluzione potrà poi essere estesa a tutti quei processi che richiedano la firma di un documento e, dal punto di vista dei soggetti coinvolti, alla rete dei promotori/agenti di cui l'Intermediario dovesse eventualmente servirsi.

Il processo messo a punto dal CSE garantisce inoltre piena affidabilità (disaster recovery), ben integrandosi nell'architettura applicativa delle Banche clienti, con tutte le funzionalità necessarie per supportare un processo privo di supporti cartacei.

Fra i principali vantaggi della soluzione, particolare rilevanza assumono:

- la gestione paperless dei processi di sportello (dematerializzazione delle contabili, della busta di cassa, ecc.);
- l'abbattimento dei costi di gestione della carta;
- la riduzione delle malversazioni nelle operazioni contabili allo sportello.

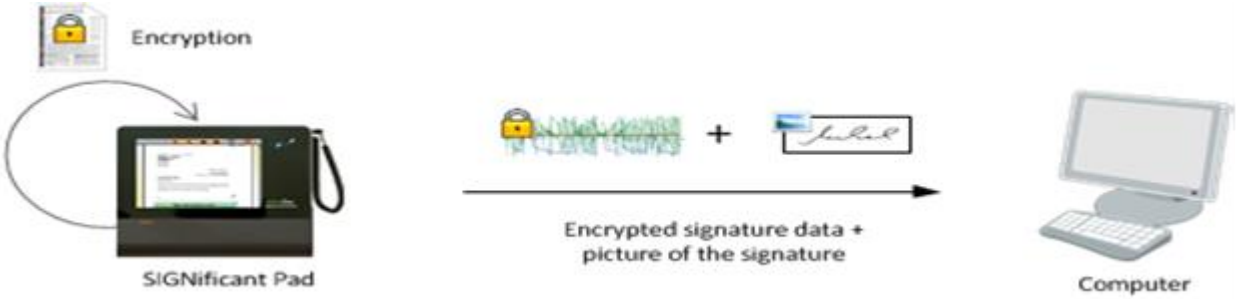
1.3. La sicurezza della firma grafometrica

Realizzare una soluzione di firma grafometrica richiede di integrare uno specifico software con dispositivi esterni (denominati tablet o signature pad), che consentono, oltre all'acquisizione della firma del cliente, la rilevazione e registrazione sia di dati statici (come l'immagine della firma), sia di dati dinamici (fra questi l'accelerazione, la velocità, l'inclinazione, la pressione ed i movimenti aerei).

Sul documento informatico così firmato sono conseguentemente memorizzate entrambe le tipologie di informazioni, statiche e dinamiche, opportunamente crittografate: l'immagine della firma viene posta in una sezione visibile, mentre i dati biometrici sono integrati nella componente informatica del documento stesso (non visibili). È evidente, a questo punto, come la sicurezza offerta dai prodotti utilizzati (hardware e software) sia un elemento qualificante per la scelta della soluzione.

Pertanto, si evidenziano di seguito alcuni punti di attenzione.

Aspetti di sicurezza inerenti la trasmissione dei dati biometrici tra il tablet (dove i dati sono stati prelevati) ed il PC ove gli stessi vengono memorizzati all'interno del documento.



L’aspetto fondamentale è rappresentato dal fatto che i dati biometrici acquisiti sul tablet vengono immediatamente protetti con una chiave di cifratura e, subito dopo l’inoltro al client, indissolubilmente legati all’impronta (hash) del documento. Dati biometrici ed impronta del documento vengono poi cifrati insieme, andando a realizzare quella che, tecnicamente, si definisce come “document binding”, ovvero una procedura in grado di dimostrare, in maniera inequivocabile, la correlazione fra documento e firma elettronica.

La firma non è così apposta su un documento in bianco ma proprio su quello che l’utente, tra l’altro, avrà avuto modo di visionare, pagina per pagina, sul tablet stesso. La cifratura consente di far sì che nessun dato viaggi mai in chiaro nella tratta tablet → PC.

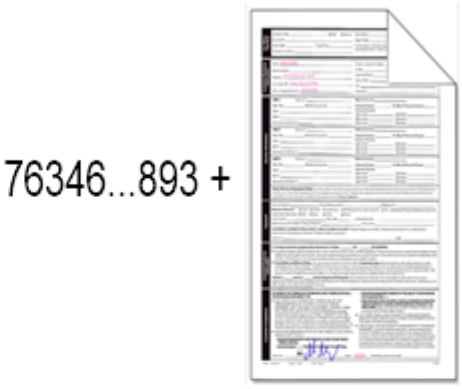
Al termine della singola operazione, tutti i dati biometrici acquisiti e trattati dal tablet vengono cancellati.

Gestione delle chiavi di cifratura

Dati biometrici ed hash del documento su cui è apposta la firma sono cifrati con una chiave pubblica, ma chi gestisce la corrispondente chiave privata, ovvero quella chiave che può essere utilizzata, in caso di contenzioso, per dimostrare l’indissolubilità tra i dati biometrici ed il documento?

La soluzione approntata prevede che la chiave privata sia sempre e comunque conservata in maniera sicura e particolarmente protetta da parte di una terza parte di fiducia: in questo modo sarà più facile, a fronte di eventuale contestazione, dimostrare che la stessa non è stata trafugata o intercettata.

Biometric signature data are encrypted with the public key of a certificate using a standardized mathematical method.



The encrypted biometric signature data are embedded invisibly into the doucment.

Seguendo queste regole, la soluzione di firma elettronica avanzata sopra descritta si configura come sicura anche agli occhi di un perito che dovesse eventualmente esaminarla in caso di disputa.

2. Processi di riconoscimento biometrico

In generale, con il termine "*riconoscimento biometrico*" ci si riferisce all'identificazione o alla verifica automatica di identità degli individui, attraverso la valutazione di caratteristiche fisiche e comportamentali.

I due distinti obiettivi di un processo biometrico sono quindi:

a) la verifica della dichiarazione di identità di un soggetto;
b) l'attribuzione di un'identità ad un soggetto.

La soluzione approntata e descritta nel presente documento rientra nel primo ambito, ossia nella verifica della dichiarazione di un'identità, in una fase ex-post (ossia a fronte di una contestazione). Non si tratta, quindi, di un tentativo di attribuzione di un'identità, posto che l'identificazione resta a cura dell'addetto bancario che si trovi al cospetto del cliente.

2.1. Accesso fisico e logico

È importante evidenziare che, quantunque sia la biometria, pur con differenti implicazioni, possa indirizzare verso due problematiche fra loro molto diverse:

1) l'accesso fisico (controllo biometrico degli accessi fisici), con procedure di accertamento della titolarità del soggetto all'ingresso di locali, edifici, comprensori, aree riservate;
2) l'accesso logico (controllo biometrico degli accessi logici), ossia accertamento della titolarità del soggetto che usufruisce di una risorsa informatica.

La soluzione di firma grafometrica rientra nel secondo gruppo (natura logica dell'accesso) e risulta rilevante per via delle implicazioni a livello di gestione della privacy.

2.2. Verifica e Identificazione

In un **processo di verifica**, normalmente detto "uno a uno", i dati acquisiti da un generico sensore biometrico vengono comparati con quelli precedentemente depositati da quel cliente (ad esempio ciò può avvenire quando si deposita, su un archivio informatico, uno specimen con la firma elettronica).

In un **processo di identificazione**, invece, i dati acquisiti dal sensore biometrico vengono comparati con un insieme di dati biometrici, di diversi clienti, contenuti in un archivio.

La definizione, nel processo informatico, di "autenticazione", ossia dell'operazione che permette di provare, nei confronti di un'applicazione, l'identità di un soggetto, trova corrispondenza, in campo biometrico, nella verifica.

Pertanto, laddove si parli, in maniera generica, di riconoscimento e/o autenticazione biometrica, si intende riferirsi ad un processo di verifica biometrica, ovvero un processo che permette la verifica di un'utenza similarmente ad altre tecnologie ad oggi in uso (es. password, codici personali, ecc.), con risultati oltremodo più attendibili.

La tabella di seguito riporta le differenze nell'utilizzo dei dati biometrici tra la modalità di identificazione e la modalità di autenticazione.

Tabella di confronto	Identificazione	Autenticazione
Acquisizione del dato biometico	Potrebbe essere passivo (utente inconsapevole)	Attiva, l'utente può decidere deliberatamente se firmare sul tablet
Qtà dati biometrici trattati	Da 1 a N , devo scandire tutti i dati registrati per verificarne la verosimiglianza	1 a 1 , confronto solo il dato biometrico dell'utente che chiede di essere autenticato
Cui Prodest ?	Un processo di identificazione può essere utilizzato per vari scopi, alcuni dei quali senza un interesse dell'utente.	Al cliente, certo che la sua identità non possa essere trafugata Alla Banca, una maggiore sicurezza contro i tentativi di frode
Ambito di Utilizzo	Potenzialmente infinito	Solo per applicazioni che richiedano una strong authentication

2.3. Biometria fisica e comportamentale

Un'ulteriore importante differenziazione, nell'ambito del riconoscimento biometrico, è relativa alla distinzione fra aspetti fisici e comportamentali.

In particolare:

1) biometria "fisica" è quella basata su dati derivati da caratteristiche fisiche dell'individuo, quali ad esempio impronte digitali, caratteristiche del viso, dell'iride o della mano;
2) biometria "comportamentale" è quella basata sulla valutazione di caratteristiche comportamentali dell'individuo, quali ad esempio il tipo di andatura, l'emissione della voce o la dinamica di apposizione della firma (quest'ultima oggetto della soluzione descritta nel presente documento).

La tecnica insita nel processo di gestione della firma grafometrica rientra quindi nella sfera della biometria comportamentale, la quale, per sua natura, non tratta dati sensibili dell'individuo, al contrario delle tecniche in grado di intercettare i dati fisici (biometria fisica).

2.4. Biometria interattiva e passiva

Il riconoscimento biometrico insito nel processo descritto nel presente documento può essere realizzato esclusivamente con clienti firmatari a conoscenza dell'operatività del sistema (biometria interattiva), che lo abbiano deliberatamente accettato come strumento di autenticazione, per quanto ex-post. Non si tratta, pertanto, di biometria passiva, la quale prevede l'uso di sistemi biometrici ad insaputa dell'utenza (ad esempio per il controllo accessi).

2.5. Riconoscimento biometrico

Tra le modalità di riconoscimento, quello biometrico si pone nel novero delle c.d. "tecniche positive", ossia quelle in cui il cliente firmatario dichiara, preventivamente, la propria identità.

La prova del legame tra la persona e l'identità in precedenza memorizzata nel sistema, su richiesta dell'interessato, si opera tramite il confronto tra le caratteristiche della firma grafometrica del campione presentato al momento e quelle della firma presente sul documento informatico in precedenza sottoscritto ed oggetto di contestazione. Si attua così una verifica ex-post della firma apposta sul documento.

2.6. Fase di verifica ex-post

Il sistema acquisisce il campione biometrico del cliente (nel nostro caso composto da dati comportamentali), che è quindi comparabile, tramite specifico software, con quello precedentemente memorizzato nella fase di firma del documento informatico (residente su un supporto di memoria di una risorsa informatica).

L'esito del confronto sarà vero/falso in funzione del superamento di una soglia prefissata (matching score) tra il campione presentato e quello in precedenza registrato e indicizzato con un codice identificativo univoco associato all'utente.

La procedura di verifica appena descritta è tipica dei sistemi di riconoscimento quale quello oggetto della presente soluzione.

2.7. Caratteristiche biometriche della firma

Poiché la firma di un individuo è ragionevolmente unica, non tanto per l'immagine della stessa ma per una serie di caratteristiche, quali ad esempio la velocità di scrittura, la pressione esercitata firmando o altri aspetti che appartengono alla sfera comportamentale e sono pressoché inimitabili, qualora la stessa non sia apposta su un foglio di carta bensì su uno speciale strumento (quale ad esempio un tablet), è possibile trasformare in dati informatici gli aspetti comportamentali, senza richiedere un cambio delle abitudini da parte dell'utente ed autenticandolo in maniera pressoché certa.

In dettaglio, i parametri comportamentali presi in considerazione per il riconoscimento biometrico della firma sono:

- la velocità di scrittura,
- la pressione esercitata,
- l'angolo di inclinazione della penna,
- l'accelerazione del movimento,
- il numero di volte che la penna viene sollevata dal tablet.

Tra i vantaggi della soluzione prospettata, vi è, come già evidenziato, l'alto grado di accettazione da parte degli utenti, che non trovano differenze significative fra il metodo tradizionale di apposizione della firma su carta e quello biometrico con firma su tablet.

3. Il processo di firma grafometrica

Prima di descrivere in dettaglio il processo di firma, è utile riepilogare i soggetti che, a vario titolo, intervengono:

- la Banca che ha optato per la soluzione di Firma Elettronica Avanzata, al fine di dematerializzare le contabili di sportello;
- il Centro servizi (CSE Consorzio Servizi Bancari) che ha sviluppato la soluzione per la Firma Elettronica Avanzata, mettendola a disposizione della Banca;
- il Cliente della Banca che aderisce al nuovo servizio, firmando le contabili "elettroniche" sul tablet;
- l'Addetto della Banca, il quale deve verificare l'identità del cliente e che, nello svolgimento delle proprie mansioni, vede sostituire la tradizionale firma su carta con l'innovativa firma sul tablet.

3.1. Flusso del processo di firma

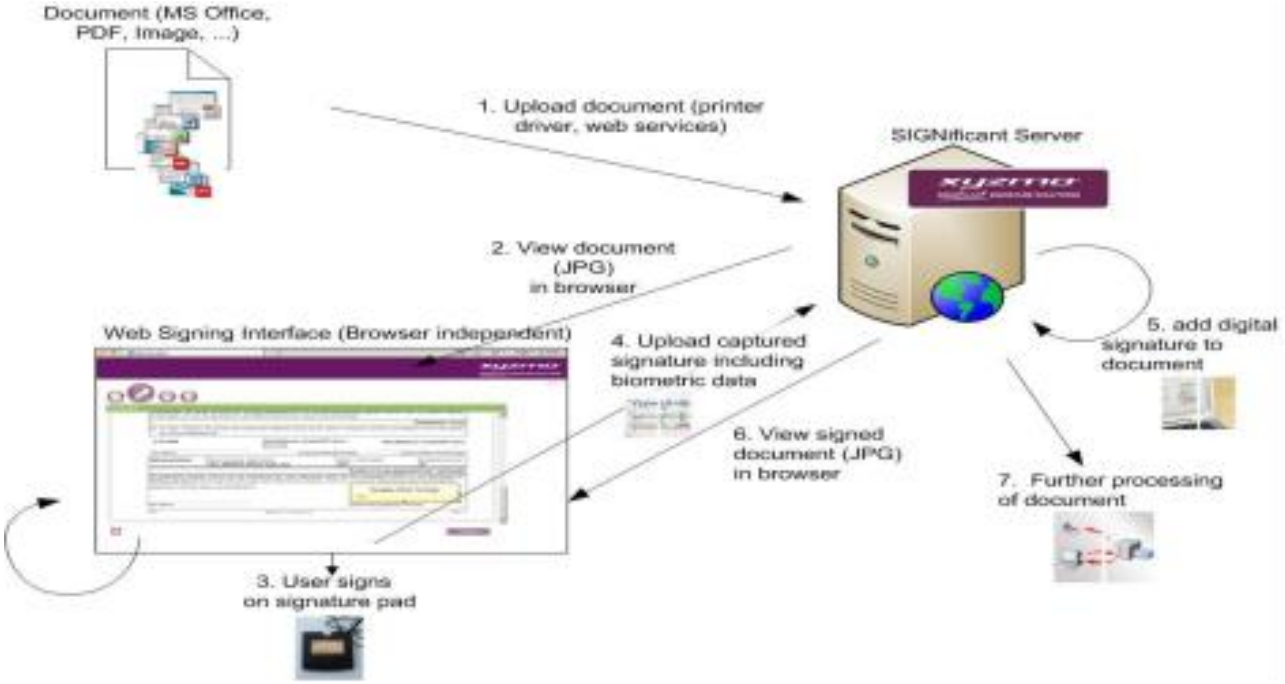
1) Il Cliente si presenta allo sportello per eseguire un'operazione che richiede la firma di una contabile;
2) l'Addetto della Banca identifica il Cliente nelle consuete modalità, procedendo poi secondo la normale operatività;
3) se l'operazione richiesta allo sportello prevede la firma di una contabile, l'Addetto della Banca informa il Cliente (se quest'ultimo non ha mai utilizzato la Firma Grafometrica) della possibilità di attivare il nuovo servizio, fornendone termini e condizioni. Quindi innesca la generazione della lettera di accettazione del servizio, chiedendo al Cliente di sottoscriverla. Se invece il Cliente ha già sottoscritto in precedenza la lettera di attivazione, si procede con il passo successivo;
4) l'immagine della contabile generata a conclusione dell'operazione (o i suoi dati essenziali) è visualizzabile dal Cliente sul tablet (oppure su uno schermo);
5) l'Addetto della Banca evidenzia il punto di firma, quindi il Cliente procede apponendo la firma sul tablet, mediante apposita penna. Sul tablet o sullo schermo è visualizzabile il documento comprensivo dell'immagine della firma;
6) il tablet acquisisce l'immagine della firma ed i dati biometrici (velocità, pressione, inclinazione, accelerazione e movimento) ad essa associati. L'abbinamento dei dati genera una Firma Grafometrica non riproducibile da persona diversa dal firmatario;
7) il tablet, man mano che acquisisce i dati, li protegge con chiave di cifratura (concordata randomicamente col driver) e li inoltra al client;
8) il driver del tablet, presente sul client, decifra (grazie alla chiave pre-concordata) i dati biometrici ricevuti, i quali vengono poi legati indissolubilmente all'impronta informatica (hash) del documento; l'intero pacchetto (dati biometrici ed hash) è infine protetto con la chiave pubblica di cifratura nota al software di Sportello (client), al fine di impedirne il successivo uso fraudolento;
9) il documento (arricchito con il pacchetto cifrato contenente i dati biometrici e l'hash) viene poi definitivamente "sigillato" con l'apposizione della firma elettronica associata alla Banca, al fine di garantirne l'integrità. Il documento così ottenuto non può essere successivamente modificato, pena l'invalidità dello stesso. Un'eventuale manomissione verrebbe difatti rilevata facilmente, anche solo con la semplice lettura del documento tramite ADOBE reader;
10) qualora il Cliente lo richieda, l'Addetto della Banca provvede alla stampa e consegna di una copia cartacea del documento, ove è visibile l'immagine della firma precedentemente

apposta sul tablet. In alternativa, è possibile inviare copia elettronica via e-mail ovvero renderla disponibile sull'internet banking riservato del Cliente;

11) il documento elettronico firmato sul tablet è pronto per essere assoggettato al processo di conservazione, come un qualunque altro documento avente firma elettronica e, lato Banca, non è stata prodotta alcuna copia cartacea.

Dal punto di vista applicativo e sistemistico, il processo operativo e funzionale descritto in precedenza è implementato utilizzando:

- una componente server (Significant Server) che risiede nel server farm del CSE e che è integrata con l'applicazione di sportello;
- un tablet collegato alla postazione della Banca, sul quale il Cliente appone la firma.



La figura sopra riportata permette di ripercorrere i vari passaggi:

I. nel momento in cui la contabile è stata predisposta e prima che venga firmata, la stessa viene inviata al Significant Server;
II. l'immagine di tale contabile (o i suoi dati salienti) viene resa disponibile sul tablet;
III. il Cliente, una volta verificati i dati della contabile, firma sul tablet;
IV. i dati biometrici catturati al momento della firma, insieme all'hash del documento, vengono ritornati (protetti con chiave di cifratura), per il tramite del client di Sportello, al Significant Server;
V. il Significant Server provvede a generare la firma elettronica Banca da apporre sul documento al fine di garantirne, nel tempo, integrità ed autenticità;
VI. il documento è sempre visualizzabile sul tablet e, a questo punto, include anche l'immagine della firma del Cliente;
VII. a conclusione del processo, il documento è pronto per la conservazione.

Nello svolgimento del processo, a fianco delle componenti puramente tecnologiche (tablet, Significant Server, applicativo di sportello), è determinante, per garantire la massima sicurezza della soluzione, l'utilizzo, in momenti diversi, di due certificati digitali: uno di cifratura per la riservatezza dei dati biometrici, uno di firma (Banca) per l'integrità e l'autenticità del documento.

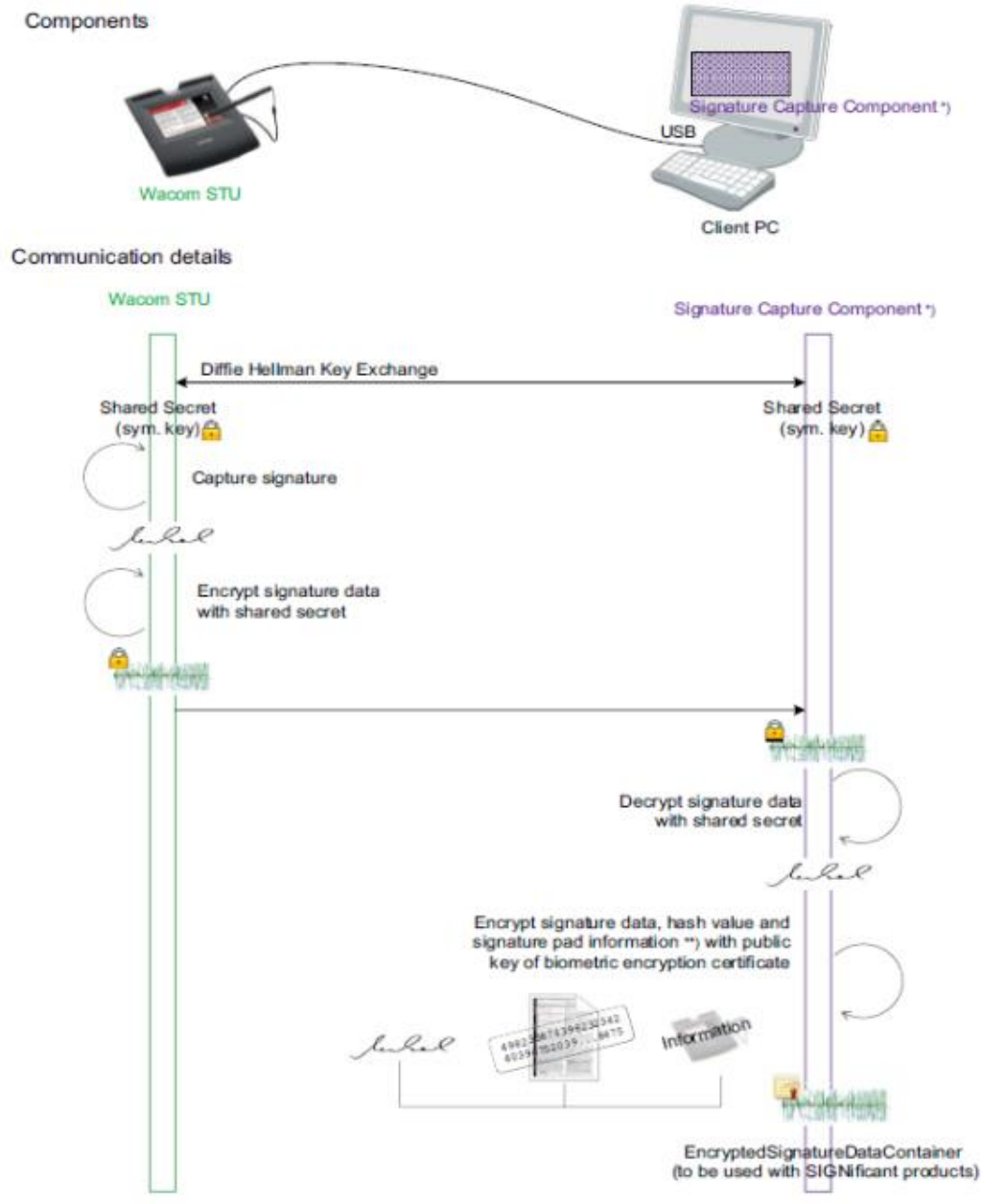
Per l'emissione di entrambi i certificati digitali, CSE si avvale dei servizi forniti dalla Certification Authority Intesa S.p.A., iscritta all'Albo dei Certificatori Accreditati gestito dall'Agenzia per l'Italia

Digitale (AgID). Le caratteristiche e le modalità di emissione e di gestione di questi certificati vengono di seguito approfondite.

3.2. Certificato di Cifratura

Il certificato di cifratura è utilizzato per proteggere i dati biometrici del Cliente, acquisiti dal tablet; quindi, trattasi di certificato che garantisce sia una sicurezza end-to-end delle comunicazioni fra postazione client e Significant Server (la comunicazione tablet-client è invece protetta da chiave randomica scambiata fra il tablet ed il suo driver presente sul client), sia il fatto che i dati biometrici raccolti (opportunamente abbinati all'impronta del documento) non possano essere utilizzati, in maniera fraudolenta, associandoli a documenti diversi da quelli per cui sono stati acquisiti.

Per schematizzare la modalità di utilizzo del certificato e della sua chiave pubblica, riportiamo la seguente figura:



*) SIGNificant Client, SIGNificant WSI Java Applet, SIGNificant .NET SDK, SIGNificant Java SDK
**) As each siganture tablet has different parameters information which tablet was used (including important characterisitics) is added to the biometric signature data. This allows a normalization of the biometric signature data for biometric authentication or manual comparison in case of trial.

Per garantire la massima sicurezza, è necessario definire come questo certificato viene emesso e reso disponibile; in particolare, massima attenzione deve essere prestata alla conservazione della chiave privata generata in corrispondenza della chiave pubblica del certificato.

Infatti, solo chi detiene tale chiave privata può decifrare i dati precedentemente protetti.

Per questo motivo è stata approntata una procedura di sicurezza, messa a punto fra la Certification Authority (INTESA S.p.A.) ed il produttore della componente software denominata Significant Server (la società austriaca XYZMO), tale da azzerare ogni rischio di uso improprio del certificato.

Il certificato di cifratura, come detto, è utilizzato per cifrare i dati biometrici raccolti dal tablet, impedendone l'accesso non autorizzato.

Tale certificato non deve necessariamente scadere in pochi anni, bensì possono tranquillamente avere validità di 20 anni o più; il punto rilevante non è difatti rappresentato dalla durata del certificato, quanto piuttosto dalla conservazione e protezione della sua chiave privata.

Per cifrare i dati biometrici e l'hash del documento, la chiave pubblica del certificato di crittografia deve essere "iniettata" nel software di Sportello, più precisamente nella componente d'interfaccia con il driver del tablet.

La coppia di chiavi di crittografia ed il certificato ad esse associato vengono generati da INTESA (in qualità di Certification Authority), la quale si incarica di consegnare la chiave pubblica, precedentemente generata, al fornitore del software (società XyZmo), per "iniettarla" nella rispettiva componente del pacchetto di Sportello.

La conservazione della chiave privata, invece, è a cura di una terza parte di fiducia.

3.3. Certificato di Firma digitale

Il certificato di firma serve per apporre, sul documento, la firma elettronica della Banca, la quale viene applicata dopo l'avvenuta associazione fra i dati biometrici della firma del Cliente e l'impronta del documento stesso, nonché dopo la cifratura di questi dati.

L'apposizione della firma Banca garantisce che il documento non possa essere manipolato e/o modificato in un momento successivo. La firma elettronica, inoltre, consente di dimostrare, in ogni momento, l'integrità del documento.

Anche il certificato in questione è rilasciato dalla predetta autorità di certificazione riconosciuta ed ha un ciclo di vita molto più breve rispetto a quello di crittografia (normalmente 3 anni).

Va detto, peraltro, che la sostituzione di tale certificato consiste in una procedura tecnica molto semplice e, da un punto di vista normativo, il cambio del certificato non invalida in alcun modo i documenti precedentemente firmati (e portati in conservazione).

Sul tema della firma digitale, si ritiene di particolare interesse segnalare che INTESA è riconosciuta, da ADOBE, all'interno di uno specifico servizio denominato AATL (Adobe Approved Trust List). INTESA ha aderito a questo servizio con la stipula di apposito contratto (a titolo oneroso), nel quale sono definite le regole che la Certification Authority deve rispettare per entrare e rimanere nel circuito; fra tali regole è inserita anche la possibilità di auditing effettuato da AgID in quanto ente regolatore italiano delle firme digitali.

Grazie al predetto servizio, i Clienti possono aprire i documenti PDF (contabili di sportello) senza dover effettuare, preventivamente, operazioni propedeutiche consistenti nell'inserimento, all'interno del proprio ADOBE Reader (o Writer), dei root certificates della Certification Authority che ha emesso il certificato di firma. Ciò evita al Cliente di:

- ricevere messaggi di errore (o warning) al momento della verifica della firma presente sui documenti;
- effettuare operazioni manuali di import di root certificates, assumendosi la responsabilità di considerare “trusted” la Certification Authority emittente il certificato di firma da verificare.