CARATTERISTICHE DELLA SOLUZIONE DI FIRMA ELETTRONICA AVANZATA

Documento predisposto ai sensi dell'Art. 57 del DPCM 22.02.2013 "Regole tecniche in materia di generazione apposizione e verifica delle firme elettroniche avanzate qualificate e digitali"

1. Informazioni generali

La **Banca di Credito Cooperativo di San Marco dei Cavoti e del Sannio Calvi** (di seguito "Banca") ha attivato una soluzione di firma grafometrica che permette ai Clienti di sottoscrivere elettronicamente i documenti in seguito elencati. Tale soluzione si inquadra nel più ampio progetto di dematerializzazione dei processi bancari che ha come finalità la progressiva sostituzione della documentazione cartacea a favore di "documenti informatici".

La sottoscrizione con firma grafometrica avviene con un processo che – nel rispetto dei requisiti normativi previsti – consente di qualificarla come Firma Elettronica Avanzata (FEA) ai sensi del Decreto del Presidente del Consiglio dei Ministri del 22.02.2013 "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali" pubblicato in GU n. 117 del 21.05.2013.

2. La firma grafometrica – che cosa è e come si attiva

La firma grafometrica è una firma che il Cliente appone di suo pugno utilizzando una "penna elettronica" e una "tavoletta digitale" (denominata anche "tablet di firma") messi a disposizione da parte della Banca, il cui utilizzo combinato consente la registrazione, oltre al tradizionale tratto grafico della firma, anche di ulteriori elementi caratteristici della sottoscrizione (dati biometrici).

Il Cliente della Banca prima di utilizzare la firma grafometrica sottoscrive, apponendo una firma "tradizionale" su un supporto cartaceo, il modulo di accettazione delle condizioni del servizio. In fase di accettazione del servizio l'utente viene identificato tramite un valido documento di riconoscimento che viene conservato a norma di legge. Il Cliente riceve adeguata informativa per il trattamento dei suoi dati personali (Data Privacy) e sottoscrive il relativo consenso.

In qualunque momento il Cliente potrà revocare l'utilizzo della firma grafometrica richiedendo presso gli sportelli della banca il modulo di cessazione.

I documenti sottoscritti dal Cliente con una Firma Elettronica Avanzata, sono documenti informatici che giuridicamente hanno lo stesso valore dei documenti cartacei sottoscritti con firma autografa.

3. Rispetto dei requisiti di Firma Elettronica Avanzata (FEA)

Per poter essere riconosciuta come Firma Elettronica Avanzata (FEA) una firma elettronica deve rispettare determinati requisiti normativi. Di seguito si indica per ciascun requisito previsto dall'Art. 56 del DPCM 22.02.2013 come esso viene soddisfatto nella soluzione messa a disposizione da parte della Banca; nel capitolo 4 si illustrano più in dettaglio le caratteristiche tecniche.

a) Identificazione del firmatario del documento

Il Cliente che firma il documento viene identificato dalla Banca, con una modalità analoga a quella prevista nell'operatività tradizionale, tramite il riconoscimento diretto da parte dell'operatore della Banca o tramite idoneo documento identificativo in corso di validità.

b) Connessione univoca della firma al firmatario

Il Cliente firma il documento tramite la penna elettronica e il tablet messi a disposizione della Banca dopo l'avvenuta identificazione da parte dell'operatore. L'operatore inoltre effettua i controlli di conformità della firma apposta mediante un confronto visivo tra l'immagine raccolta dal tablet e quella depositata in precedenza in modo analogo a quanto avviene per una firma autografa.

I dati biometrici della firma sono associati in modo sicuro, protetto e con garanzia di integrità al documento informatico. I dati raccolti racchiudono informazioni potenzialmente superiori rispetto alla firma autografa su carta e – tramite un processo rigorosamente definito – possono essere verificati (perizia grafica) da un soggetto incaricato dall'Autorità Giudiziaria, nonché per le altre finalità previste dalla legge. La Banca non può, in nessun caso, autonomamente consultare i dati biometrici presenti nel documento.

c) Controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima

Nella fase di apposizione della firma sul tablet il Cliente ha il controllo fisico del dispositivo; può verificare le informazioni visualizzate sullo schermo del tablet, scorrere i contenuti del documento che poi verrà sottoscritto e apporre autonomamente la firma. Durante la sottoscrizione, il tablet permette di vedere in tempo reale il segno grafico tracciato e, se necessario, il Cliente può effettuare l'annullamento dell'operazione di firma e ripetere la sottoscrizione.

Tutto il processo e le componenti tecniche che costituiscono il sistema di firma sono improntate a garantire un elevato livello di sicurezza che coinvolge l'hardware messo a disposizione, le componenti software utilizzate e le fasi di colloquio tra di esse, la modalità di gestione dei dati e le relative logiche di protezione. Più in dettaglio il tablet è realizzato con una struttura che ne garantisce l'integrità da compromissioni; tutti i dati trasmessi nel processo di firma sono sempre protetti (anche nei riguardi del personale della Banca) con adeguati meccanismi di crittografia e non possono essere riutilizzati successivamente.

d) Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma

Terminata la fase di sottoscrizione del documento da parte del Cliente, il sistema provvede ad includere nel documento stesso i dati biometrici crittografati della firma che quindi sono univocamente collegati al documento. Il documento informatico viene sigillato in modo automatico dal sistema software che ne garantisce l'integrità nel tempo.

e) Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto

Prima della sottoscrizione il Cliente può consultare il contenuto del documento direttamente sul dispositivo tablet. Successivamente alla sottoscrizione, il Cliente può:

- ricevere in modalità elettronica un documento in formato PDF quale attestazione di quanto sottoscritto tramite il servizio di pubblicazione su web in area riservata (servizio InBank – area InfoBanking) se il Cliente si avvale di tale servizio;
- richiedere la stampa del documento.

f) Individuazione del soggetto che eroga la soluzione di firma elettronica avanzata

La Banca è il soggetto che, ai sensi dell'Art. 55, comma 2, lettera a) del DPCM 22.02.2013, eroga la soluzione di Firma Elettronica Avanzata (FEA). La soluzione è realizzata avvalendosi di società specializzate e dotate dei requisiti necessari ed è integrata con il sistema informativo della Banca.

g) Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati

Il processo di firma è improntato a criteri di automazione, sicurezza e affidabilità che garantiscono l'integrità dei documenti sottoscritti. Il documento informatico è generato e predisposto per la sottoscrizione nel formato ISO/IEC PDF/A.

h) Connessione univoca della firma al documento sottoscritto

I dati biometrici della firma sono automaticamente memorizzati nel documento informatico con una modalità che li collega univocamente all'impronta informatica del documento stesso. Queste informazioni sono protette con algoritmi crittografici al fine di garantire, oltre che la riservatezza, l'impossibilità di estrazione o duplicazione dei dati biometrici.

La dichiarazione di accettazione all'utilizzo della firma grafometrica

L'utilizzo della firma grafometrica con valore di firma elettronica avanzata avviene dopo che il Cliente ha accettato, con un'apposita dichiarazione, di utilizzare questa modalità di firma.

Il Cliente può chiedere in ogni momento, gratuitamente, una copia della suddetta dichiarazione di accettazione da lui firmata, contestualmente o successivamente al momento della firma.

Questa richiesta può essere fatta, per iscritto, alla Filiale della Banca a cui la dichiarazione è stata rilasciata.

4. Descrizione delle caratteristiche tecnologiche della soluzione

Le informazioni riferite alla firma sono trattate con le seguenti modalità:

a) Il tratto grafico della firma (e solo quello) è visualizzato all'operatore di sportello e può essere confrontato visivamente con l'immagine depositata in precedenza (specimen) per l'effettuazione dei controlli di conformità previsti.
b) Le informazioni biometriche rilevate:
   - la pressione della penna sul display;
   - le coordinate del tratto tra cui anche i tratti in cui la penna viene sollevata (tratti in aria);
   - il tempo con cui si esegue la firma;

   sono protetti sin da quando sono fisicamente raccolte sul tablet e crittografate all'interno del documento elettronico sottoscritto.
c) Le informazioni quali:
   - la velocità con cui si esegue la firma;
   - l'accelerazione durante la fase di scrittura;

   sono invece calcolati durante la fase di estrazione dei dati dallo strumento a disposizione del grafologo.

La connessione tra il tablet di firma e la postazione di lavoro dell'operatore bancario avviene in modalità protetta utilizzando l'algoritmo AES con chiave generata dinamicamente e scambiata secondo l'algoritmo DIFFIE-HELLMAN-MERKLE.

I dati biometrici crittografati prima di essere inseriti nel documento sono ulteriormente protetti tramite crittografia con un certificato tecnico a chiave asimmetrica (con algoritmo RSA) e con l'uso di algoritmi di hashing di tipo SHA.

I dati biometrici non vengono in nessun modo memorizzati in chiaro, né dal tablet, né dall'applicazione di firma. L'insieme dei dati biometrici viene inoltre connesso, in modo univoco ed indissolubile al documento informatico del Cliente, in modo che la stessa firma grafometrica non possa essere associata ad un altro documento.

Inoltre, al fine di garantire l'integrità, l'intero documento firmato dal Cliente, a "sigillo" di ogni documento viene aggiunta una firma tecnica riconducibile alla Banca.

Il documento digitale sottoscritto dal Cliente e con i dati biometrici crittografati viene memorizzato nel formato ISO/IEC PDF/A e firmato tecnicamente in modalità PAdES (ETSI TS 102 778) attraverso l'applicazione di una firma digitale tecnica, basata su un ulteriore certificato con chiave privata ed algoritmo RSA in modo da soddisfare i requisiti normativi legati all'autoconsistenza, integrità e leggibilità dello stesso.

La Banca non può in alcun modo accedere ai dati biometrici del Cliente e, la decifratura degli stessi, può avvenire esclusivamente nel rispetto di un protocollo stabilito tra la Banca e una Certification Authority (Ente Certificatore accreditato) che emette il certificato di cifratura in qualità di TSP (Trust Service Provider). L'accesso può avvenire solo per il tramite di un soggetto incaricato dall'Autorità Giudiziaria (es. Perito Calligrafico CTU), nonché per le altre finalità previste dalla legge, e necessita congiuntamente della messa a disposizione delle credenziali di accesso da parte della Banca e da parte della Certification Autority (che quindi singolarmente non sono mai in grado di attivare il processo). L'analisi forense dei dati biometrici contenuti nel documento avviene tramite uno specifico software messo a disposizione dalla Certification Authority.

5. Valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità

Finalità

I dati biometrici sono raccolti e trattati per l'esclusiva finalità di sottoscrizione conforme ai requisiti legali della forma scritta e secondo le regole tecniche della FEA.

Le finalità sono descritte e autorizzate dal Cliente in sede di adesione al servizio di FEA tramite l'informativa conforme all'articolo 57, comma 1, lettera a) del d.P.C.M. 22 febbraio 2013.

Necessità

Nella soluzione adottata, i dati personali biometrici sono utilizzati al solo scopo di sottoscrivere con il soddisfacimento del requisito della forma scritta i documenti informatici proposti dalla Banca e autorizzati dal Cliente in sede di adesione al servizio di FEA tramite l'informativa conforme all'articolo 57, comma 1, lettera a) del d.P.C.M. 22 febbraio 2013.

I dati biometrici grezzi sono cancellati immediatamente e nella forma di sottoscrizione biometrica sono accessibili solo su richiesta dell'autorità giudiziaria e secondo le regole stabilite nel Provvedimento.

Proporzionalità

Il sistema di rilevazione dei dati biometrici è configurato solo per l'acquisizione dei dati indispensabili per l'apposizione di una sottoscrizione informatica conforme ai requisiti minimi legali della FEA.

Le informazioni inerenti alla posizione (compresi i cosiddetti salti in volo), al tempo, e alla pressione del segno grafometrico vengono raccolte in modo assolutamente "acritico" e trasformate in una stringa di dati binari, senza che, in alcun caso, le suddette caratteristiche possano essere analizzate – nemmeno incidentalmente – al fine di risalire ad informazioni che potrebbero riguardare lo stato di salute dell'interessato.

Nel caso di patologie motorie inerenti l'instabilità del tratto nel tempo le informazioni della sottoscrizione sono identiche a quelle grafiche desumibili da una sottoscrizione cartacea.

6. Ulteriori informazioni

La Banca ha stipulato, in ottemperanza a quanto previsto dall'Art. 57, comma 2, la prevista polizza assicurativa per la responsabilità civile con primaria assicurazione abilitata ad esercitare nel campo dei rischi industriali.

7. Tipologie di documenti sottoscrivibili con Firma Elettronica Avanzata

Di seguito si precisano le tipologie di documenti che sono sottoscrivibili, alla data di pubblicazione del documento, con Firma Elettronica Avanzata:

- Ordini di bonifico e giroconto;
- Ordini di pagamento deleghe fiscali;
- Disposizioni di prelevamento e compravendita valuta;
- Distinte di versamento e cambio assegni;
- Altre disposizioni/ordini di pagamento (es. bollette);
- Quietanza pensione;
- Richieste e ricevute per emissione carnet assegni;
- Richieste di costituzione di deposito vincolato (con firma unica);
- Questionari MiFID;
- Consulenza, schede prodotto, preordini e ordini titoli;
- Questionari KYC singoli e multipli.