

## Scheda tecnica illustrativa della soluzione di Firma Elettronica Avanzata (FEA)

Il presente documento descrive le caratteristiche del sistema e delle tecnologie utilizzate per la gestione della soluzione di Firma Elettronica Avanzata (di seguito FEA) della Banca, e costituisce parte integrante e sostanziale delle Condizioni Generali di servizio a cui l'Utente sottoscrittore (cfr. art. 1.2 delle CGS) è tenuto ad aderire per poter usufruire del servizio medesimo.

Si tratta di una tecnologia innovativa che permette ai clienti e ai loro delegati di firmare la documentazione intercorrente con la Banca in formato elettronico eliminando così l'uso della carta.

Chi accetta di utilizzare questa modalità visualizza e firma il documento su uno strumento denominato tablet mediante un'apposita penna elettromagnetica.

La soluzione adottata dalla Banca è stata realizzata in conformità al decreto legislativo n. 82/2005 (Codice dell'Amministrazione Digitale e successive modifiche), al D.P.C.M. del 22 febbraio 2013, "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali" e al Provvedimento del Garante per la Protezione dei dati personali n. 513 del 12 novembre 2014 che disciplinano la materia.

I documenti informatici validamente sottoscritti mediante la soluzione FEA producono gli effetti previsti dalla legislazione vigente, e segnatamente: a) a norma dell'art. 21 comma 2 del CAD, hanno la stessa efficacia probatoria dei documenti cartacei sottoscritti ex art. 2702 c.c.; b) a norma dell'art. 21 comma 2-bis del CAD, soddisfano il requisito della forma scritta per gli atti di cui all'art. 1350 n. 13 c.c..

L'Utente ha il diritto di ottenere, in qualsiasi momento liberamente e gratuitamente sul supporto da lui prescelto (cartaceo o elettronico), copia delle CGS dallo stesso sottoscritte e della presente Scheda Tecnica Illustrativa. Per ottenere tale documentazione il firmatario può rivolgersi alla filiale di riferimento o all'indirizzo di posta elettronica indicato nelle CGS.

Il firmatario può in ogni momento recedere dal servizio comunicando la sua volontà a mezzo di lettera raccomandata ovvero a mezzo di dichiarazione scritta rilasciata al dipendente della Banca che ne accuserà ricevuta.

### **La soluzione di firma elettronica avanzata proposta**

Il sistema di sottoscrizione proposto si basa sulla raccolta, cifratura e conservazione, unitamente al documento sottoscritto, dei dati biometrici legati al comportamento tenuto in fase di sottoscrizione e che permettono, successivamente, ed esclusivamente in caso di contestazione, di dimostrare l'imputabilità della sottoscrizione al soggetto che l'avesse disconosciuta.

### **Caratteristiche del sistema**

La soluzione è orientata alla sicurezza delle informazioni trattate, ne garantisce l'integrità, la leggibilità dei dati e l'inalterabilità, impedendo ogni possibile accesso abusivo ai dati stessi.

L'utilizzo di documenti informatici, in sostituzione di quelli cartacei, avviene mediante la tecnologia che permette agli Utenti del servizio di consultare i documenti riguardanti le operazioni disposte allo sportello su un apposito schermo (tablet) e sottoscriverli a conferma delle operazioni disposte, in modo semplice e simile all'apposizione di una firma autografa tradizionale. Questo particolare tipo di firma elettronica avanzata ("firma grafometrica") permette il rilevamento dinamico dei dati calligrafici della firma, idonei a rilevare le caratteristiche di seguito indicate, oltre al segno grafico, che costituiscono i "dati biometrici" relativi alla firma del sottoscrittore:

- coordinate x e y (sono i punti in cui la penna viene appoggiata allo schermo per comporre la firma)
- pressione della penna e sua inclinazione
- velocità con cui si esegue la firma
- accelerazione durante la fase di scrittura
- tempo

Il dato biometrico dei sottoscrittori di documenti informatici, viene acquisito mediante l'interoperabilità di componenti hardware e software. La cifratura dei dati biometrici avviene con le modalità indicate nel successivo paragrafo denominato "La connessione univoca della firma al documento sottoscritto".

### **L'identificazione del firmatario del documento**

La Banca identifica il firmatario con un documento di riconoscimento in originale e in corso di validità al momento dell'adesione al servizio.

### **La connessione univoca della firma al firmatario**

La soluzione di firma proposta si basa sull'acquisizione dei dati biometrici/comportamentali statici e dinamici legati all'azione della sottoscrizione.

La connessione univoca della firma al firmatario è garantita:

- dall'identificazione certa del firmatario da parte dell'operatore della Banca
- dal fatto che la firma è apposta dal firmatario di suo pugno con penna elettromagnetica sul tablet in presenza dell'operatore della Banca

### **La garanzia del controllo esclusivo del firmatario del sistema di generazione della firma**

Durante la fase di firma il sistema è sotto il controllo esclusivo del firmatario. Il tablet mostra il documento informatico completo (o i dati principali dell'operazione se trattasi di operazioni contabili effettuate allo sportello), consentendo al firmatario di verificare personalmente i propri dati e il contenuto del documento informatico con scorrimento. Durante l'apposizione della firma, il tablet rappresenta in tempo reale il segno grafico tracciato (tratto grafico della firma). La Banca può conoscere esclusivamente l'immagine della firma, senza la possibilità di accedere, o comunque, di utilizzare i dati biometrici in chiaro.

### **La possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma**

L'integrità e l'inalterabilità del documento informatico sono garantite dall'inserimento dei dati biometrici (criptati) del firmatario nel documento informatico in formato pdf e dalla successiva criptazione del documento informatico con le modalità indicate nel successivo paragrafo denominato "La connessione univoca della firma al documento sottoscritto".

La verifica della firma grafometrica (ad esempio a seguito di un disconoscimento della sottoscrizione avvenuto in giudizio) sarà possibile decriptando i dati biometrici e confrontandoli con quelli raccolti in giudizio dal perito incaricato, che effettuerà le proprie comparazioni secondo regole non dissimili a quelle utilizzate negli attuali processi di verifica di sottoscrizioni su carta. Affinché tutto il processo possa offrire idonee garanzie per entrambe le parti (Cliente e Banca), la chiave (privata) necessaria per decifrare correttamente i dati biometrici è affidata ad una terza parte fidata e indipendente (la Certification Authority identificata e selezionata dall'outsourcer informatico BCC Sistemi Informatici) in grado di garantirne la corretta custodia. Solo ed esclusivamente ove a ciò autorizzata dalla Banca, su richiesta del cliente o di un pubblico ufficiale, per esclusive esigenze di verifica di una firma disconosciuta, la Certification Authority effettuerà, in ambiente sicuro, la decifrazione dei dati biometrici e ne sorveglierà l'utilizzazione da parte del perito incaricato dalle Autorità Competenti, curando anche che al termine delle operazioni peritali, si proceda alla cancellazione sicura di tutti i dati elaborati.

### **La possibilità per il firmatario di ottenere evidenza di quanto sottoscritto**

Il firmatario può richiedere alla Banca una copia cartacea del documento con cui ha disposto l'operazione oppure, in alternativa, ricevere copia del documento in formato elettronico tramite il servizio di rendicontazione on line (disponibile per i Clienti titolari dei servizi di internet banking).

In tutti i casi i documenti possono essere recuperati, consultati, stampati, anche su richiesta del soggetto interessato, durante tutto il periodo di conservazione.

### **Individuazione del soggetto erogatore della soluzione di firma elettronica avanzata**

I servizi sono resi dalla Banca in qualità di soggetto che eroga la soluzione di firma elettronica avanzata al fine di utilizzarla nei rapporti intrattenuti con gli Utenti.

### **Assenza nell'oggetto della sottoscrizione di qualunque elemento idoneo a modificarne gli atti, i fatti e i dati in esso rappresentati**

Il documento informatico prodotto è in un formato pdf firmato elettronicamente tale da impedire l'inserimento all'interno dello stesso di programmi o istruzioni potenzialmente atti a modificare gli atti, fatti o dati rappresentati nel documento medesimo (es. macro).

### **La connessione univoca della firma al documento sottoscritto**

La soluzione di firma proposta si basa sull'acquisizione dei dati biometrici/comportamentali statici e dinamici legati all'azione della sottoscrizione.

Al fine di garantire la connessione univoca della firma grafometrica al documento, l'applicazione di firma:

- calcola per il documento generato dalla transazione, prima dell'apposizione sullo stesso della firma, una stringa di numeri e lettere (tramite c.d. algoritmo di "hash"), quale elemento univoco di identificazione del documento prodotto
- riceve dalla tavoletta in maniera sicura (criptata) i dati biometrici della firma (sia "statici" che "dinamici") e li abbina alla stringa calcolata in precedenza, creando un c.d. "blog di firma"
- "chiude" e cifra il blog di firma (creata in precedenza) tramite un processo di crittografia asimmetrica; una chiave è detenuta dalla Banca (denominata "chiave pubblica") e una è conservata a cura di un soggetto terzo rispetto alla Banca (denominata "chiave privata", necessaria per decodificare il blog di firma criptato). Il soggetto che detiene la chiave privata è la Certification Authority

identificata e selezionata dall'outsourcer informatico BCC Sistemi Informatici, cui sono vengono impartite vincolanti istruzioni dalla Banca relativamente all'uso della chiave privata per le sole finalità indicate nel paragrafo denominato "La possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma"

- sul documento ottenuto, nel quale esiste un riferimento cifrato sia al documento precedente la firma (stringa alfanumerica) che al firmatario (dati biometrici), calcola un nuova stringa univoca (con un algoritmo di "hash") e
- nel caso di distinta contabile chiude il documento con la chiave privata di una coppia di chiavi asimmetriche generate a nome dell'outsourcer informatico e dallo stesso detenute;
- nel caso di contratto chiude il documento con il certificato digitale del funzionario delegato della Banca, rilasciato da una Certification Authority riconosciuta;
- Infine, il documento informatico viene portato in Conservazione Digitale presso ICCREA Banca.

Il suddetto legame univoco costruito tramite sistema di cifrature, impedisce che il vettore biometrico di firma possa essere estratto e riutilizzato su un altro documento, in quanto resta sempre riconducibile all'unico documento cui è collegato, firmato originariamente dal cliente.

Il documento potrà essere decifrato, in caso di necessità, per l'esibizione in giudizio o su richiesta dell'autorità giudiziaria, su richiesta del cliente o per esigenze della Banca per la verifica dell'integrità del contenuto dello stesso e della paternità della firma apposta, solo con il concorso del possessore della chiave "privata".

### **Copertura assicurativa**

Come previsto dalla normativa vigente, la Banca ha stipulato una polizza assicurativa - rilasciata da primarie compagnie di assicurazione abilitate ad esercitare nel campo dei rischi industriali - per la responsabilità civile da danno a terzi eventualmente derivante dalla fornitura del servizio di FEA.