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) e costituisce parte integrante e sostanziale delle Condizioni Generali di Servizio (nel seguito, CGS) a cui l'Utente sottoscrittore (cfr. art. 1.2 delle CGS) è tenuto ad aderire per poter usufruire del servizio medesimo (nel seguito Utente).
Si tratta di una tecnologia innovativa che permette ai clienti e ai loro delegati di firmare la documentazione intercorrente con ogni singolo Erogatore in formato elettronico, eliminando così l'uso della carta.
L'Utente che accetta di utilizzare questa modalità visualizza e firma il documento su uno strumento denominato tablet mediante un'apposita penna elettromagnetica.
La soluzione adottata dalla Erogatori 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 agli Erogatori ai recapiti indicati nelle Condizioni generali di Servizio, al punto 4.3.
L'Utente 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 anche in nome e per conto di Iccrea Banca S.p.A..

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 della firma, idonei a rilevare le caratteristiche di seguito indicate, oltre al segno grafico, che costituiscono i "dati biometrici" relativi alla firma dell'Utente:

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

Il dato biometrico degli Utenti che sottoscrivono documenti informatici tramite la soluzione FEA 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 dell'Utente del documento

La Banca in epigrafe, anche in nome e per conto di Iccrea Banca, identifica l'Utente con un documento di riconoscimento in originale e in corso di validità al momento dell'adesione al servizio. Inoltre, copia del documento di riconoscimento in corso di validità al momento dell'adesione al servizio verrà conservata secondo le modalità descritte nelle CGS (punto 5.2).

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 all'Utente è garantita:

- dall'identificazione certa dell'Utente da parte dell'operatore della Banca (anche in nome e per conto di Iccrea Banca)
- dal fatto che la firma è apposta dall'Utente di suo pugno con penna elettromagnetica sul dispositivo in presenza dell'operatore della Banca in epigrafe

La garanzia del controllo esclusivo dell'Utente del sistema di generazione della firma
Durante la fase di firma il sistema è sotto il controllo esclusivo dell'Utente. Il dispositivo 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 dispositivo rappresenta in tempo reale il segno grafico tracciato (tratto grafico della firma). Gli Erogatori possono conoscere esclusivamente l'immagine della firma, senza alcuna 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) dell'Utente 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 (Utente e Erogatori), 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, con la quale la Banca in epigrafe ed Iccrea Banca hanno, ognuna per quanto di ragione, un rapporto contrattuale diretto avente ad oggetto il rilascio della coppia di chiavi asimmetriche e l'attività di c.d. Key recovery della chiave privata) in grado di garantirne la corretta custodia. Solo ed esclusivamente ove a ciò autorizzata dagli Erogatori, 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 decifratura 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 l'Utente di ottenere evidenza di quanto sottoscritto
L'Utente può richiedere agli Erogatori una copia cartacea, o elettronica, del documento con cui ha disposto l'operazione, come indicato alle CGS (punto 4.2). 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 epigrafe e da Iccrea Banca in qualità di Erogatori della soluzione FEA al fine di utilizzarla nei rapporti intrattenuti da ognuna 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, la soluzione FEA:

- 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 (creato con le modalità di cui al punto precedente) tramite un processo di crittografia asimmetrica, utilizzato dal realizzatore della soluzione di firma, BCC Sistemi Informatici, nell'interesse della Banca in epigrafe e di Iccrea Banca S.p.A. che all'uopo mettono a disposizione dello stesso la propria chiave pubblica per la cifratura automatica dei predetti blob di firma. La corrispondente chiave privata, senza la quale il blob di firma non può essere "aperto", è conservata a cura di un soggetto terzo. In particolare, il soggetto che detiene la chiave privata è la Certification Authority identificata e selezionata dall'outsourcer informatico BCC Sistemi Informatici, con la quale la Banca in epigrafe ed Iccrea Banca intrattengono un rapporto contrattuale diretto avente ad oggetto il rilascio della coppia di chiavi asimmetriche e la c.d. procedura di Key recovery, ed a cui vengono impartite vincolanti istruzioni 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) sia all'Utente (dati biometrici), calcola un nuova stringa univoca (con un algoritmo di "hash") e

  - nel caso di distinta contabile, con riferimento alla Banca in epigrafe, 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 dell'incaricato delegato della Banca, anche in nome e per conto di Iccrea Banca, rilasciato da una Certification Authority riconosciuta;

- Infine, il documento informatico (sia che si tratti di documento relativo al rapporto tra l'Utente e la Banca in epigrafe, sia che riguardi il rapporto tra l'Utente ed Iccrea Banca), viene portato in Conservazione Digitale presso un conservatore a ciò autorizzato. Ove tale soggetto sia identificato dalla BCC in epigrafe in ICCREA Banca, la stessa conserva i dati in ambienti separati a seconda se siano riconducibili a rapporti Utente/Banca o Utente/Iccrea Banca medesima.

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 dall'Utente.
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 degli Erogatori 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, Gli Erogatori hanno stipulato ognuno 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.