BPER:
Gruppo

Manuale del Gruppo BPER del Processo di Firma Elettronica Avanzata (FEA)

V. 3 del 10/02/2016

Sommario

1 Introduzione e Scopo

Il presente documento ha lo scopo di descrivere il Servizio di Firma Elettronica Avanzata (FEA), strutturato come Firma Grafometrica, che il Gruppo BPER ha sviluppato, nell'ambito del progetto "Paperless – La Green Bank", con l'obiettivo di automatizzare l'attività di generazione, sottoscrizione ed archiviazione della documentazione prodotta dalle filiali, ottimizzando il processo e garantendone il rispetto anche nell'ottica di una riduzione dei rischi operativi e legali.
L'obiettivo è quello di gestire in modalità completamente dematerializzata sin dall'origine (generando documenti informatici), non solo le contabili prodotte dallo sportello di cassa ma anche altre tipologie di operazioni e documenti (es. contabili di bonifico, questionario di adeguata verifica, etc) e di contratti.
L'ambito di applicazione è quello di uno scenario di utilizzo di dispositivi di tipo grafometrico (Signature Pad) in tutte le postazioni di cassa ed in alcune postazioni di front-office delle Filiali del Gruppo BPER.
Il progetto firma grafometrica si pone l'obiettivo di adottare un sistema di riconoscimento della firma autografa del cliente in modo sicuro ed opponibile a terzi secondo le disposizioni recate dal CAD – Codice dell'Amministrazione Digitale di cui al D.Lgs. n. 82/2005 in materia di Firma Elettronica Avanzata (FEA) e del D.P.C.M. 22 febbraio 2013, attuativo del Codice, recante le regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.

Più precisamente, l'articolo 21 del CAD disciplina compiutamente il valore probatorio di un documento informatico sottoscritto, prevedendo che quando gli sia stata apposta una firma elettronica qualificata o digitale oppure anche una firma elettronica avanzata, acquista di per sé un'efficacia probatoria pari a quella della scrittura privata ai sensi dell'articolo 2702 del codice civile. Costituisce quindi piena prova sino a querela di falso della provenienza delle dichiarazioni di chi l'ha sottoscritto.

La firma elettronica avanzata, a differenza di quella qualificata e di quella digitale, non necessita né di un certificato qualificato né di un dispositivo sicuro per la sua valida apposizione. La definizione del CAD opera infatti solamente un generico riferimento ai mezzi di cui il firmatario dispone e su cui esercita un controllo esclusivo[1].

Di fatto la Firma Elettronica Avanzata (FEA) non è che una firma elettronica con alcune caratteristiche di sicurezza. Diversamente dalla firma elettronica qualificata e dalla firma digitale, la definizione di Firma Elettronica Avanzata (FEA) non comporta l'uso necessario di una determinata tecnologia. La Firma Elettronica Avanzata (FEA) è infatti un processo rispetto a cui è necessario accertare, caso per caso, se sono soddisfatti i requisiti indicati dalla norma, quali le caratteristiche del sistema di apposizione della firma, le modalità attraverso cui l'utente appone la firma, le modalità di memorizzazione dei parametri biometrici della firma, la possibilità di verificare che il documento non abbia subito alterazioni dopo l'apposizione della firma e la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto.

Il documento sottoscritto con firma grafometrica ha pertanto valore equivalente a quello firmato in modo tradizionale (con firma autografa). Il Servizio di Firma Elettronica Avanzata (FEA) si può applicare ai documenti contabili ed ai contratti verso la Clientela, con la sola eccezione di quelli aventi ad oggetto beni immobili, di cui all'art.1350, primo comma, nn. da 1 a 12, del Codice Civile.

La soluzione di Firma Elettronica Avanzata, descritta all'interno del presente Manuale, è stata realizzata in conformità e ai sensi e per gli effetti delle prescrizioni in materia di privacy dettate in tema di biometria dal Provvedimento n. 513 del 26.11.2014 del Garante per la Protezione dei Dati Personali.

[1] *La firma elettronica avanzata è, in particolare, "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".*

2 Termini e Definizioni

Caratteristica biometrica	caratteristica biologica o comportamentale di un individuo da cui possono essere estratti in modo ripetibile dei tratti biometrici (biometric features) distintivi e idonei al riconoscimento biometrico
Riconoscimento biometrico	si intende il riconoscimento automatico di individui basato su loro caratteristiche biologiche o comportamentali
Campione biometrico (biometric sample)	rappresentazione analogica o digitale di una caratteristica biometrica ottenuta al termine del processo di acquisizione (biometric capture e biometric acquisition)
Documento informatico	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Firma Elettronica Avanzata	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
Soluzioni di Firma Elettronica Avanzata	soluzioni strumentali alla generazione e alla verifica della firma elettronica avanzata
Firma grafometrica	particolare tipo di Firma Elettronica Avanzata (FEA) che si ottiene dal rilevamento “dinamico” dei dati calligrafici della firma, effettuata con penna elettronica su Signature Pad dotati di appositi pannelli per la cattura del tratto grafometrico del firmatario.
Firma digitale	un particolare tipo di Firma Elettronica Avanzata (FEA) basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Identificazione informatica	la validazione dell’insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l’individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell’accesso
Chiave privata	l’elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico
Chiave pubblica	l’elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche
Certificato X509	certificato che rispetta la struttura definita nello standard X.509 (standard ITU-T per le infrastrutture a chiave pubblica)
Sistema crittografico a chiave simmetrica	la crittografia simmetrica è un tipo di crittografia dove ogni attore coinvolto nella comunicazione dispone della medesima chiave; tale chiave viene usata sia per la cifratura del messaggio in chiaro sia per la decifratura del messaggio cifrato.
Sistema crittografico a chiave asimmetrica	la crittografia asimmetrica (nota anche come crittografia a coppia di chiavi, crittografia a chiave pubblica/privata o crittografia a chiave pubblica) è un tipo di crittografia dove ad ogni attore coinvolto nella comunicazione è associata una coppia di chiavi: la chiave pubblica, che deve essere distribuita, serve a cifrare un documento destinato alla persona che possiede la relativa chiave privata; la chiave privata, personale e segreta, utilizzata per decifrare un documento cifrato con la chiave pubblica; evitando così il problema connesso alla distribuzione delle chiavi
Conservazione elettronica	sistema che assicura, dalla presa in carico dal produttore fino all’eventuale scarto, la conservazione, tramite l’adozione di regole, procedure e tecnologie, dei documenti informatici in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità secondo le regole stabilite dal D.P.C.M. 3.12.2013 e dal D.M. 17.6.2014 per i documenti a rilevanza fiscale

3 Ruoli

Cliente e/o Firmatario	il soggetto che ha aderito al Servizio di Firma Elettronica Avanzata
Banca	soggetto che eroga soluzioni di firma elettronica avanzata – FEA ai sensi e per gli effetti dell'art. 55, comma 2, lett. a) del D.P.C.M. 22.2.2013. Nella specie, la soluzione di FEA è erogata al fine di utilizzarla nei rapporti intrattenuti con la Clientela avvalendosi di una soluzione realizzata da un soggetto "Terzo"
Soggetto Terzo	soggetto che realizza una soluzione di FEA per conto della Banca; la soluzione è stata attivata dalla Società di Servizi del Gruppo Bper, Bper Services S.c.p.A., avvalendosi del software di firma ENSoft prodotto da Euronovate S.A.
Operatore	soggetto incaricato dalla Banca della realizzazione delle seguenti attività: raccolta dei dati anagrafici ed acquisizione del documento di riconoscimento; raccolta del consenso all'adesione del Servizio di firma; riconoscimento del soggetto (secondo obblighi di legge) e di assistenza tecnico operativa al firmatario nelle attività di firma
Terza parte fidata	soggetto (Notaio) incaricato dalla Banca, depositario della chiave privata. L'esternalizzazione del Servizio è stata gestita secondo la normativa vigente al momento della sottoscrizione
Conservatore	soggetto incaricato dalla Banca per la conservazione a norma di legge dei propri documenti. L'esternalizzazione del Servizio è stata gestita secondo la normativa vigente al momento della sottoscrizione

4 Componenti Tecnologiche del processo di firma

Signature Pad	tavoletta grafica USB con display da 10" in grado di riprodurre l'intero template da sottoscrivere, utilizzato per catturare il tratto grafometrico della firma
Dispositivo scanner	scanner in grado di acquisire, a sistema, copia del documento di identità del Cliente che intende aderire al Servizio di Firma Elettronica Avanzata
Server di Firma	Dispositivo collegato in modalità https alle postazioni dotate di Signature Pad; è deputato: - alla gestione del documento informatico prodotto; - all'inserimento nello stesso dei dati grafometrici "dinamici" (dati biometrici) e "statici" (immagine) opportunamente cifrati per permetterne al firmatario un controllo esclusivo e una connessione univoca allo specifico documento firmato (Blob dei Dati Grafometrici cifrato); - all'apposizione della Firma Digitale con certificato qualificato per chiavi crittografiche emesso da una Certificaton Authority (CA) e custodito su dispositivi sicuri di firma condivisi (HSM – Hardware Security Module) e conformi alla norma tecnica UNI CEI ISO/IEC 27001:2005, così da rendere immodificabile il PDF/A; - all'invio del documento PDF/A in conservazione a norma presso il Conservatore; - all'invio della copia del documento firmato priva di dati biometrici (c.d. flatten) nel sistema documentale della Banca; - della messa a disposizione al Cliente della propria copia dei documenti firmati FEA, secondo la modalità indicata dallo stesso in sede di adesione al Servizio.
Applicazione Web Documentale della Banca	Procedura per la conservazione, ricerca e consultazione dei documenti informatici senza dati biometrici (c.d. copia "flatten")

5 Contesto normativo di riferimento

Tale paragrafo è volto a indicare sinteticamente la normativa di riferimento emanata dall'Autorità di Vigilanza (Consob, Banca d'Italia) e/o normativa primaria (a titolo esemplificativo: leggi, decreti legge, decreti legislativi, Codice Civile, etc.). Di seguito si fornisce indicazione sintetica della normativa esterna di riferimento:

- D.Lgs. del 7 marzo 2005 n. 82 - Codice dell'amministrazione digitale, pubblicato nella Gazzetta Ufficiale 16 maggio 2005, n. 112, S.O. ;
- D.P.C.M. del 22 luglio 2011 - Comunicazioni con strumenti informatici tra imprese e amministrazioni pubbliche, ai sensi dell'articolo 5-bis del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni, pubblicato nella Gazzetta Ufficiale 16 novembre 2011, n. 267;
- D.P.C.M. 22.2.2013 - Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20. Comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71, pubblicato nella Gazzetta Ufficiale 21 maggio 2013, n. 117;
- D. Lgs. N. 196/2003 (Codice in materia di protezione dei dati personali);
- Provvedimento Generale Garante Privacy in tema di Biometria n.513 del 12/11/2014.

6 Descrizione del Servizio

Il Servizio di Firma Elettronica Avanzata (FEA) permette la sottoscrizione di documenti informatici attraverso l'utilizzo di dispositivi di cattura del tratto grafometrico (Signature Pad) che consentono di rilevare le caratteristiche dinamiche distintive di una firma autografa (i c.d. dati grafometrici).
In alcune postazioni di lavoro sono installate specifiche Signature Pad, dotate di apposite "penne", su cui la Clientela, una volta identificata a norma di legge e a conclusione delle operazioni effettuate, può apporre la propria firma. Le Signature Pad, tramite il particolare software, sono in grado di catturare i dati grafometrici del tratto di firma del cliente (ritmo, velocità, pressione, accelerazione, movimento), informazioni che verranno memorizzate all'interno dei documenti informatici sottoscritti, in forma cifrata tramite sistemi di crittografia a chiave pubblica con certificato digitale emesso da un certificatore accreditato ai sensi dell'art. 29 del Codice dell'amministrazione digitale. I documenti saranno conservati elettronicamente a norma di legge.
Pertanto, una volta apposta sulla Signature Pad la firma grafometrica da parte del Cliente (anche richiedendo al Cliente di apporre tante firme grafometriche quanti sono i campi richiesti, così come accade su supporto cartaceo), questa viene visualizzata sulla Signature Pad per la conferma da parte del Cliente.
La Signature Pad invia, in modo sicuro con protocollo di comunicazione https, il dato al server di firma.

Più nel dettaglio, i dati grafometrici raccolti tramite la Signature Pad vengono cifrati in modo tale da permetterne al firmatario un controllo esclusivo e una connessione univoca allo specifico documento firmato; l'applicazione di firma inserisce quindi i dati grafometrici "dinamici" (dati biometrici) e "statici" (immagine) nel file PDF/A, che viene poi reso immodificabile attraverso l'apposizione di una Firma Digitale con certificato Banca emessa da una Certification Authority (CA) e portato in conservazione a norma.
In ragione della struttura stessa del processo, la firma grafometrica apposta dal Cliente diviene non più utilizzabile su ulteriori e diversi documenti in quanto associata in maniera inscindibile al documento cui è apposta (binding tra firma cliente e documento); considerando il fatto che la firma grafometrica è assistita da una serie di caratteristiche (velocità, pressione, inclinazione …) uniche e mai riproducibili da un soggetto diverso dal firmatario effettivo, ne consegue che non sarà possibile utilizzare la firma di un soggetto in luogo di un altro.

Il processo è costruito quindi in maniera tale da assicurare la non riutilizzabilità della firma grafometrica apposta dal Cliente a documenti diversi da quello sottoscritto.
In questo senso il processo descritto è in linea con tale requisito in quanto il dato biometrico non viene mai salvato su hardware ma risulta presente, in maniera cifrata (criptata), solamente sul documento finale.
Inoltre, a livello di sicurezza, la cifratura dei dati e l'utilizzo di un doppio sistema di cifratura a chiave asimmetrica (uno per la cifratura e l'altro per la firma del PDF/A) impedisce che il dato "catturato" possa essere utilizzato per scopi diversi ed ulteriori.

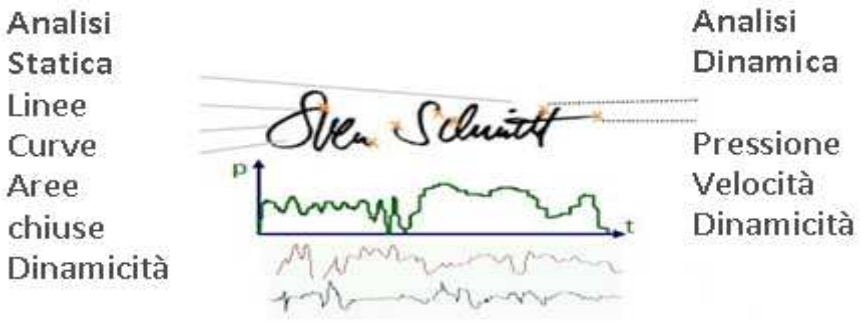
Al Cliente che aderisce al Servizio Firma Elettronica Avanzata (FEA) è data facoltà di ricevere copia della documentazione (contabile/contratto) di sua spettanza secondo le seguenti 4 modalità:

- Elettronica nell'apposita Area presente in Posta On Line dell'Internet Banking SMART e Web/CBI;
- Elettronica tramite posta elettronica;
- Elettronica tramite Posta Elettronica Certificata (di prossima attivazione);
- Cartacea.

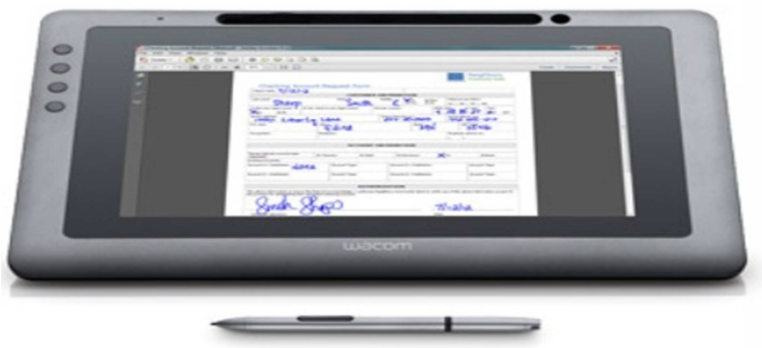
Indipendentemente dalla modalità scelta dal cliente in sede di adesione, è sempre data facoltà al medesimo di richiedere copia cartacea del documento all'operatore al termine dell'operazione effettuata.

7 Firma Grafometrica – definizione

La Firma Grafometrica è un particolare tipo di Firma Elettronica Avanzata (FEA) che si ottiene dal rilevamento "dinamico" dei dati calligrafici della firma, effettuata con penna elettronica sulla Signature Pad dotati di appositi pannelli per la cattura del tratto grafometrico del firmatario.
Il software a bordo della Signature Pad rileva i 5 tratti caratteristici della firma autografa (ritmo, velocità, pressione, accelerazione, movimento), generando il c.d. blob dei dati biometrici:



I tratti rilevati dalla Signature Pad di Firma vengono criptati e divengono parte integrante del documento informatico che viene reso immodificabile e conservato a norma di legge per un numero di anni secondo quanto previsto dalla vigente normativa.
L'hardware utilizzato è costituito da una Signature Pad USB con monitor 10" che costituisce un vero e proprio monitor da tavolo in grado di riprodurre l'intero modulo da sottoscrivere e di catturare il tratto biometrico della firma.



8 Processo di Esercizio di Firma Grafometrica (in sintesi)

Il processo di esercizio ovvero l'applicazione della Firma Elettronica Avanzata (FEA) come firma grafometrica ai documenti da sottoscrivere, si svolge nelle seguenti fasi:

- autenticazione dell'Operatore Banca al Sistema di Firma attraverso credenziali personali;
- riconoscimento del Firmatario e verifica dell'esistenza di un'adesione attiva al Sistema di FEA;
- illustrazione del Servizio al Cliente da parte dell'Operatore Banca;
- eventuale compilazione del modulo di adesione al servizio FEA nel caso il Firmatario non abbia ancora aderito, allegando copia elettronica di un documento di identità in corso di validità;
- produzione, in formato elettronico, del documento da sottoscrivere;
- presa visione del documento da sottoscrivere da parte del Firmatario sulla Signature Pad;
- sottoscrizione del documento da parte del Firmatario attraverso la Signature Pad;
- invio del Blob Crittografato al Server tramite canale sicuro;
- formazione del Blob dei Dati Grafometrici cifrato;
- aggiunta del Blob Crittografato al documento .pdf sottoscritto;
- firma Digitale del produttore del documento informatico (Banca), sottoscritto dal Firmatario (c.d. firma "di chiusura");
- invio del documento informatico prodotto (PDF/A) al Responsabile della Conservazione a norma;
- invio della copia del documento informatico prodotto (priva del blob grafometrico) al sistema documentale della Banca per future ricerche e per la messa a disposizione al Cliente anche in un momento successivo dei documenti informatici sottoscritti a mezzo FEA;
- consegna al Firmatario del documento informatico sottoscritto secondo la modalità da lui scelta in fase di adesione al Servizio.

9 Processo di Adesione al Servizio di Firma Elettronica Avanzata

L'adesione al Servizio di Firma Elettronica Avanzata (di seguito FEA) è facoltativa e può essere revocata in qualsiasi momento. Laddove il Firmatario non ne accettasse le condizioni in ogni loro parte, il processo di sottoscrizione dei documenti verrà comunque realizzato in modalità tradizionale (e quindi "su carta").
Il Cliente per usufruire del Servizio deve prestare la propria adesione firmando l'apposito Modulo di Adesione prodotto da una specifico applicativo Banca.
Prima di procedere all'adesione, il Firmatario, da parte dell'Operatore Banca viene:

- identificato a norma di legge,
- adeguatamente informato riguardo alle modalità di fruizione del Servizio (comprese le limitazioni d'uso) ed al trattamento dei dati biometrici rilevati dall'apposizione della firma elettronica,

La registrazione dell'Adesione al Servizio da parte del Firmatario e l'elezione della modalità con cui ricevere la propria copia sono effettuate su uno specifico applicativo, a cui è demandata anche la scansione del documento di identità del Firmatario e la generazione del modulo di Adesione che sarà firmato con Firma Elettronica Avanzata.
L'adesione al Servizio può essere prestata dalle sole persone fisiche relativamente alle operazioni da loro sottoscritte, indipendentemente dal rapporto sul quale operano.
Il Cliente attraverso la sottoscrizione dell'adesione manifesta la volontà di aderire al Servizio, accetta la modalità di trattamento dei dati personali (ad integrazione dell'informativa sul trattamento dei dati personali che la Banca ha a suo tempo fornito al Cliente ai sensi dell'art. 13 del Codice in materia di protezione dei dati personali) ed indica la modalità di messa a disposizione della propria copia del documento sottoscritta a mezzo FEA.

L'adesione viene prestata da ogni singola persona fisica per la sottoscrizione di operazioni di sportello, documenti e contratti effettuata in qualità di:

1. **Titolare di rapporto, di operazione, di obbligazione** contratta nei confronti della Banca;
2. **Cointestatario di rapporto, di operazione, di obbligazione** contratta nei confronti della Banca, indipendentemente dal fatto che l'altro/tutti gli altri intestatario/i abbia/no a sua/loro volta accettato le condizioni del Servizio FEA;
3. **Delegato ad operare su rapporto di altro Titolare persona fisica**, indipendentemente dal fatto che il Titolare abbia a sua volta accettato le condizioni del Servizio di FEA;
4. **Soggetto legittimato legalmente ad operare su rapporto di altro Titolare persona fisica** (a titolo meramente esemplificativo e non esaustivo: procuratore speciale, procuratore generale, tutore, curatore, amministratore di sostegno), indipendentemente dal fatto che quest'ultimo abbia a sua volta accettato le condizioni del Servizio di FEA;

5. **Delegato ad operare su rapporto di altro Titolare persona giuridica e/o rappresentante legale/soggetto legittimato legalmente** ad operare su rapporto di altro Titolare persona giuridica;
6. **Presentatore occasionale e/o delegato di cassa**, indipendentemente dal fatto che il Titolare abbia a sua volta accettato le condizioni del Servizio di FEA.

Con riguardo ai soli documenti informatici sottoscritti con FEA in qualità di quanto indicato ai precedenti punti 1, 2, 3 e 4, il Cliente sceglie in fase di adesione con quale modalità riceverli secondo le seguenti 4 modalità:

- **Elettronica nell'apposita Area presente in Posta On Line** (Internet Banking SMART e Web/CBI): la copia cliente delle contabili, documenti e contratti sarà prodotta solo elettronicamente e sarà visibile dal cliente all'interno dell'area Documenti del suo Internet Banking SMART/ Web/CBI dal giorno successivo.
- **Elettronica tramite posta elettronica**: la copia cliente delle contabili, documenti e contratti sarà prodotta solo elettronicamente e messa a disposizione come allegato ad una mail generata ed inviata dal sistema entro 24 ore all'indirizzo indicato dal cliente in sede di adesione al Servizio FEA. L'invio delle e-mail avverrà solo dopo la conclusione di un processo di verifica dell'indirizzo di posta elettronica indicato dal cliente. Nello specifico, all'indirizzo indicato dal cliente in sede di adesione verrà inviata una e-mail contenente un link da attivarsi a cura dello stesso, con finalità di mera verifica. Fino a verifica avvenuta (indirizzo certificato), in deroga a quanto richiesto dal cliente, la sua copia sarà prodotta in formato cartaceo e consegnata allo sportello.
- **Cartacea:** qualora il cliente scelga tale modalità, la sua copia sarà sempre prodotta in formato cartaceo; il sistema stamperà in automatico la sola copia cliente. Poiché il cliente ha aderito al Servizio FEA, la copia Banca sarà dematerializzata.
- **Elettronica tramite Posta Elettronica Certificata** (di prossima attivazione): la copia cliente delle contabili, documenti e contratti sarà prodotta solo elettronicamente e messa a disposizione come allegato ad una mail PEC generata ed inviata dal sistema entro 24 ore all'indirizzo di posta elettronica estrapolato dalle seguenti fonti:
    - Camera di Commercio: l'indirizzo è presente negli archivi Banca grazie all'allineamento periodico del Sistema informativo con CERVED;
    - da quanto dichiarato dal cliente in sede di adesione alla FEA: l'indirizzo dichiarato dal cliente è memorizzato negli archivi Banca utilizzando l'applicazione web dedicata (qualora all'interno del sistema informativo non sia presente l'indirizzo PEC Camera di Commercio).

  Qualora il soggetto comunichi alla Camera di Commercio un nuovo indirizzo o una variazione di quello precedentemente depositato, attraverso l'allineamento automatico dell'anagrafe generale della Banca con CERVED, verrà acquisito il nuovo indirizzo e tutte le comunicazioni saranno inviate a questo. L'invio delle e-mail PEC non certificate da Cerved avverrà solo dopo la conclusione di un processo di verifica dell'indirizzo di posta elettronica indicato dal cliente. Nello specifico, all'indirizzo indicato dal cliente in sede di adesione verrà inviata una e-mail contenente un link da attivarsi a cura dello stesso, con finalità di mera verifica. Fino a verifica avvenuta (indirizzo certificato), in deroga a quanto richiesto dal cliente, la sua copia sarà prodotta in formato cartaceo e consegnata a sportello.

Con riguardo ai soli documenti informatici sottoscritti con FEA in qualità di quanto indicato al precedente **punto 5**, saranno messi a disposizione secondo le modalità scelte dal Titolare persona giuridica che abbia aderito al Servizio di messa a disposizione dei documenti a Firma Elettronica Avanzata. In caso di mancata adesione, i documenti saranno resi disponibili esclusivamente in modalità cartacea.

Con riguardo infine ai soli documenti informatici sottoscritti con FEA in qualità di quanto indicato al precedente **punto 6** saranno resi disponibili esclusivamente in modalità cartacea. indipendentemente dalla modalità scelta dal cliente in sede di adesione.

In qualsiasi momento il cliente può modificare le scelte effettuate per quanto attiene sia la modalità di messa a disposizione della propria copia, sia l'adesione al Servizio. L'eventuale revoca non produce alcun effetto rispetto all'eventuale adesione manifestata dal Titolare del rapporto (se diverso) o dal cointestatario.

Il processo di sottoscrizione dei documenti attraverso l'uso FEA dichiarazione i documenti attraverso l'uso di FEA è subordinato ai seguenti passi operativi:

- **Informativa al Cliente**: l'Operatore Banca illustra al Firmatario tutte le caratteristiche e le modalità di fruizione del Servizio (comprese le limitazioni d'uso), incluso il trattamento dei dati biometrici rilevati dall'apposizione della firma elettronica. Dette informazioni sono parte integrante del modulo di adesione e del presente manuale, a disposizione della clientela sul sito web della Banca.

- **Identificazione del Firmatario**: l'Operatore Banca ha la responsabilità di identificare in modo certo il Firmatario prima che questo possa aderire al Servizio di FEA. L'identificazione avviene mediante esibizione di un documento di identità in corso di validità con riconoscimento "de visu". Il documento di identità esibito, dopo le verifiche necessarie, viene acquisito mediante dispositivo scanner al fine di essere conservato assieme alla dichiarazione di adesione, a norma di legge.
- **Scelta della modalità di messa a disposizione della copia cliente**: l'Operatore Banca richiede al Cliente la modalità con cui intende ricevere copia della documentazione da lui sottoscritta, scelta fra quelle tempo per tempo messe a disposizione dalla Banca (e-mail, Smart/CBI, cartacea e, di prossima attivazione, e-mail PEC) e la registra nell'applicativo Banca.
- **Sottoscrizione dell'adesione**: una volta identificato il Firmatario, scelta la modalità di messa a disposizione della copia Cliente e raccolta copia elettronica di un documento di identità in corso di validità, l'applicativo Banca genera il modulo di adesione al Servizio di FEA ed attiva il processo di firma. Viene visualizzata l'anteprima del documento sul monitor dell'Operatore Banca, che con apposito comando trasferisce il controllo della Signature Pad al Firmatario, così che questi possa:
    - prendere visione del modulo scorrendo le pagine sullo schermo usando l'apposito pennino;
    - procedere alla sottoscrizione, toccando con l'apposito pennino lo schermo in corrispondenza del campo firma del modulo. Si aprirà un "box di firma" dove dovrà apporre la propria firma e confermarla (o ripeterla o annullarla) per terminare l'attività sul Signature Pad.

  Per consentire il controllo del documento firmato, questo viene visualizzato sul monitor dell'Operatore Banca, che dovrà quindi cliccare su "conferma (oppure su "ripeti firma" per far ripetere la firma al Cliente, oppure su "annulla" per ritornare nella mappa principale dell'applicativo di adesione). In automatico si aprirà una finestra di riepilogo contenente:
    - l'informazione della modalità scelta dal cliente (Smart/CBI, e-mail, cartacea e, di prossima attivazione, e-mail PEC) l'immagine del modulo firmato dal Cliente e, in forma digitale, dalla Banca;
    - Il pulsante "Stampa", per stampare una copia cartacea, indipendentemente dalla modalità scelta dal Cliente;
    - Il pulsante "Chiudi", che l'Operatore Banca dovrà cliccare per concludere il processo di Firma FEA allo sportello.

La copia "Banca" del modulo, unitamente ai dati grafometrici della firma del Cliente, non viene stampata ma memorizzata elettronicamente ed inviata in conservazione secondo la normativa vigente. Il documento viene conservato elettronicamente a norma di legge nella sua forma di PDF/A dal Responsabile della Conservazione.
La copia "Cliente" viene invece messa a disposizione secondo la scelta da questi effettuata in fase di adesione. Su richiesta del cliente, indipendentemente dalla scelta effettuata, l'Operatore Banca può stampare il documento in forma cartacea al termine dell'operazione effettuata.
Copia cartacea del documento può essere richiesta dal Cliente in ogni momento presso qualsiasi dipendenza della Banca a titolo gratuito.

10 Operazione di generazione, consegna e conservazione delle chiavi (pubblica e privata)

La Procedura di generazione, consegna e conservazione di chiavi di crittografia sono svolte davanti ad un Notaio, il quale ne documenta la fasi predisponendo un "verbale di constatazione e deposito".
Tali operazioni sono svolte alla presenza, oltre che del Notaio depositario, anche del Legale Rappresentante della Banca o un suo delegato e del Responsabile dell'Ufficio Gestione Sicurezza Informatica della Banca (di seguito denominato "l'esperto").
L'esperto, dopo aver constatato che la stanza in cui sono svolte le operazioni costituisce "ambiente sicuro", esibisce un involucro, aperto in presenza del Notaio, contenente un Personal Computer nella sua confezione originale di fabbrica "sigillato" e quindi mai usato.
Procede all'apertura ed accensione, per la prima volta di tale computer, su cui fa verificare ai presenti che non è installato alcun programma ad eccezione del sistema operativo Windows.
L'esperto, dopo aver constatato lo spegnimento di tutte le apparecchiature poste all'interno della stanza dotate di bluetooth e wifi e di assenza di altri strumenti di memorizzazione e ripresa, procede all'inserimento nel personal computer di un Compact Disc (CD) non riscrivibile contenente il programma di generazione chiavi. Genera la coppia di chiavi ("chiave privata" e "chiave pubblica")[2] utilizzando la procedura contenuta nel CD di generazioni chiavi inserito nel computer.

[2] *A seconda del Software utilizzato per il processo di cifratura del dato grafometrico le chiavi pubblica e privata possono essere inserite all'interno di un Certificato X509*

Al termine dell'operazione di generazione, l'esperto procede alla riproduzione della "chiave privata" generata stampandola su supporto cartaceo, masterizzandola su Compact Disc non riscrivibile e su chiave USB, tutti in duplice originale.
L'esperto procede poi alla riproduzione della "chiave pubblica" generata masterizzandola su Compact Disc non riscrivibile, in duplice originale.
Al fine di evitare che siano intercettati e/o riprodotti i dati generati durante la procedura di generazione, l'esperto, coadiuvato dal Notaio, procede alla cancellazione sicura (standard DoD) di tutti i dati contenuti nel disco fisso del Personal Computer.
Il Legale Rappresentante della Banca (o un suo delegato) consegna al Notaio tutti i supporti di memorizzazione della chiave privata, richiedendo al Notaio la custodia degli stessi in nome e per conto della Banca da lui rappresentata ed in virtù di apposito contratto di servizio. I supporti consegnati al Notaio sono quindi riposti all'interno di due buste chiuse con sigillo e sottoscrizione del Notaio lungo il bordo di chiusura, ciascuna delle quali riporta l'intestazione del Notaio e la ragione sociale della Banca – Progetto Paperless.
Le buste saranno custodite separatamente dal Notaio in due luoghi distinti, entrambi in ambienti dotati di impianto di allarme anti intrusione, ambedue all'interno di una cassaforte.
Il Legale Rappresentante della Banca (o un suo delegato) consegna quindi all'esperto tutti i supporti di memorizzazione della chiave pubblica, che dovrà poi essere depositata, da parte degli uffici competenti, sul Server di Firma per essere utilizzata nel sistema crittografico a chiave asimmetrica.
Il Notaio rilascia apposito "verbale di constatazione e deposito" del processo svolto e del ritiro delle buste contenenti i supporti di memorizzazione per la custodia.

11 Gestione del dato grafometrico

Il processo di seguito descritto raccoglie alcuni dati personali del cliente, nel rispetto delle disposizioni vigenti in materia di privacy, ovvero la relativa caratteristica biometrica (caratteristica biologica o comportamentale di un individuo da cui possono essere estratti in modo ripetibile dei tratti biometrici distintivi e idonei al riconoscimento biometrico). L'uso di opportune tecnologie e processi garantisce un elevato grado di tutela di tali dati, che non rientrano mai nella disponibilità del cliente stesso.
In particolare, i dati grafometrici raccolti tramite la Signature Pad transitano in modalità cifrata utilizzando algoritmi di cifratura "standard" [3] fino alla fase di generazione del blob biometrico cifrato.
Si precisa inoltre che:

- il dato grafometrico non è in alcun modo memorizzato su supporti permanenti della postazione di lavoro o del dispositivo di firma;
- il dato grafometrico non viene in alcun modo utilizzato per verifica o confronto con specimen depositati, ma solo codificato e memorizzato per una eventuale futura verifica;
- il cliente riceve copia del documento generato e ha la possibilità di segnalare eventuali problemi o situazioni anomale;
- la Banca e il soggetto depositario della chiave privata (la terza parte fidata cioè il Notaio) non possono accedere in autonomia al dato grafometrico in chiaro;
- il dato grafometrico è a disposizione per eventuali accertamenti solo nei casi previsti dalle attuali normative, ad esempio nell'ipotesi di una controversia, in cui il dato grafometrico può essere disponibile solo previa autorizzazione/richiesta dell'autorità giudiziaria

11.1 Blob dei Dati Biometrici

Il contenuto e le modalità con cui viene formato il blob dei dati biometrici del Firmatario soddisfano il requisito di controllo esclusivo del Firmatario del sistema di firma, richiesto dall'art. 56 par. 1 Lett. C) del D.P.C.M. 22.2.2013 recante le regole tecniche delle Firme Elettroniche.
Le fasi del processo di formazione del Blob dei dati biometrici sono le seguenti:

- Acquisizione delle grandezze fisiche principali
- Calcolo delle grandezze fisiche derivate
- Composizione del Blob Biometrico
- Cifratura del Blob Biometrico

[3] *Si intende l'insieme dei sistemi crittografici a chiave simmetrica o asimmetrica noti pubblicamente e ritenuti sicuri in quanto esenti da vulnerabilità conosciute (ad es. AES, RSA, …)*

11.2 Calcolo delle grandezze fisiche derivate

Una volta acquisite le grandezze fisiche principali, il Servizio di Firma Elettronica Avanzata (FEA) calcola le seguenti grandezze derivate:

- Movimento del Gesto di Firma, ovvero cambio di direzione del Tratto di Firma;
- Velocità del Tratto di Firma, ovvero la velocità puntuale del Tratto di Firma;
- Accelerazione del Tratto di Firma, ovvero la variazione puntuale di Velocità del Tratto di Firma;
- Ritmo del Tratto di Firma, ovvero l'alternanza di Pause e Tratti;
- Pressione del tratto di firma.

11.3 Composizione e cifratura del Blob Biometrico

Ottenute le grandezze rilevate e derivate, il Servizio di Firma Elettronica Avanzata (FEA) procede alla composizione del pacchetto di dati qui definito blob biometrico contenente: i dati Grafometrici e l'impronta del documento da sottoscrivere.
Le librerie software utilizzate nella soluzione di Firma Elettronica Avanzata (FEA) non consentono la memorizzazione, neppure temporanea, dei dati grafometrici né del blob biometrico in chiaro.

Una volta composto il blob biometrico, il Servizio di Firma Elettronica Avanzata (FEA) cifra il contenuto utilizzando apposito algoritmo. Il dato grafometrico crittografato viene associato al documento sottoscritto, tramite il suo inserimento come meta-dato del documento stesso. Tale documento viene reso statico e firmato digitalmente con il certificato intestato al Direttore Generale della Banca o ad altra persona da lui delegata.

L'intero processo garantisce:

- il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati grafometrici eventualmente utilizzati per la generazione della firma medesima;
- la connessione univoca della firma al documento sottoscritto.

Il processo di gestione delle chiavi di cifratura dei dati grafometrici è articolato nelle seguenti macro attività:

- Generazione delle chiavi: attraverso un processo codificato in presenza del Notaio viene generata la coppia di chiavi (pubblica e privata);
- Uso della chiave pubblica: la chiave pubblica viene utilizzata per la cifratura dei dati grafometrici;
- Conservazione della chiave privata: la Terza Parte Fidata (Notaio) conserva la chiave privata con modalità che garantiscano la massima sicurezza ed il pieno controllo di ogni accesso. Le informazioni sono conservate su supporti completamente isolati dagli accessi esterni.

12 Requisiti di sicurezza

Quando un documento è firmato con FEA, i dati grafometrici non sono accessibili, modificabili o riutilizzabili. Il processo prevede che i dati grafometrici siano cifrati "all'origine" prima di essere incorporati nel documento in formato PDF. La comunicazione tra PC e tavoletta avviene in modalità cifrata tramite algoritmi "standard" appositamente scelti a seconda del dispositivo utilizzato.

Dopo aver incorporato i dati grafometrici cifrati nel documento, questo è firmato digitalmente (con un certificato qualificato) rilasciato al Direttore Generale della Banca o ad altra persona da lui delegata; in questo modo il documento è reso "non modificabile".

Inoltre i dati grafometrici, anche se cifrati all'interno di un documento in formato PDF, non possono essere estratti e riutilizzati per un altro documento.
I requisiti di sicurezza correlati al Servizio di Firma Elettronica Avanzata (FEA) garantiscono quindi la:

- protezione dei dati grafometrici: il processo prevede che i dati grafometrici siano cifrati "all'origine" con algoritmi di cifratura "standard" prima di essere incorporati nel documento: vale a dire che, una volta firmato un documento, i dati grafometrici non sono accessibili in chiaro, modificabili o riutilizzabili;
- immodificabilità del documento: una volta incorporati i dati grafometrici criptati all'interno del documento in formato pdf, il documento viene firmato digitalmente. In questo modo, esso è reso "non modificabile". L'immodificabilità del documento può essere verificata con Adobe Reader: aprendo il file in formato pdf viene immediatamente mostrato un avviso, nel caso in cui il file sia

stato modificato dopo l'apposizione della firma;
- non riutilizzabilità dei dati grafometrici: i dati grafometrici, anche se cifrati all'interno di un file in formato pdf, non possono essere estratti e riutilizzati per un altro documento.

La Banca ha adottato misure ed accorgimenti in materia di sicurezza delle informazioni e dei dati secondo specifiche Linee Guida, Policy e Regolamenti, in ottemperanza alla normativa esterna vigente, con particolare riferimento alla Data Governance e Data Quality (sviluppata nell'ambito della Circolare Banca d'Italia n°263), relativamente al fatto che:

- sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione delle postazioni informatiche e dei dispositivi, se non esplicitamente autorizzati.
- I sistemi informatici sono protetti contro l'azione di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati.

13 Verifica della Firma Grafometrica

La Banca, solamente nei casi previsti dalla legge ed esclusivamente su richiesta delle autorità competenti (nello specifico in caso di contenzioso legale correlato al disconoscimento della firma), attiva una specifica procedura che consente di accedere al blob biometrico e di analizzarne i valori.

Più nel dettaglio, a seguito della cifratura del blob grafometrico l'accesso alle informazioni in esso contenute è possibile solamente mediante l'utilizzo della chiave privata da parte della terza parte fidata depositaria della stessa, e solamente a fronte di una richiesta da parte dell'autorità giudiziaria in caso di contestazioni circa l'autenticità e origine (disconoscimento) della firma grafometrica apposta.

In questo caso, dopo che la Banca ha fornito al Notaio l'originale del documento depositato in conservazione a norma si attiva una procedura software, così articolata:

- estrazione del dato grafometrico crittografato dal documento;
- richiesta al Notaio della chiave privata;
- generazione del dato grafometrico in chiaro;
- salvataggio, da parte del Notaio, del dato grafometrico in chiaro per successive verifiche.

Tale procedura è a disposizione di chi effettua la verifica per essere a sua volta verificata, in modo tale che non possano esserci contestazioni sulle modalità tecniche di gestione del dato.
La procedura tiene altresì distinte e separate le interazioni tra i diversi soggetti per evitare qualsiasi trasferimento di informazioni tra gli stessi; il dato grafometrico in chiaro deve essere accessibile solo al soggetto che effettua la verifica.
Il Notaio incaricato dell'utilizzazione della chiave privata decifra il dato grafometrico criptato in un ambiente di certificazione notarile di proprietà e sotto il suo esclusivo controllo.

Le attività di cui sopra avvengono nel rispetto dei requisiti di cui appresso:

a) il Notaio responsabile, su richiesta del giudice per il controllo autografo del documento, estrae il dato grafometrico, sotto il suo esclusivo controllo di guisa che si possa procedere alle operazioni descritte nelle lettere "b)" e seguenti, garantendo che:
    1. tutti i dati e le applicazioni siano accessibili solo sotto il controllo del Notaio;
    2. sia esclusa ogni possibilità di copiare, duplicare o alterare i dati;
    3. tutti gli applicativi e i dati contenuti nel supporto hardware sono cancellati in modo sicuro, di guisa che sia impossibile recuperarli successivamente;
    4. ogni operazione effettuata sul sistema sia monitorata e loggata;
    5. il log di tutte le operazioni sia inalterabile in quanto immediatamente firmato digitalmente dal Notaio per essere allegato al verbale delle operazioni.
b) il Notaio utilizza la chiave privata;
c) il Notaio genera una evidenza informatica con il contenuto in chiaro dei dati grafometrici contenuti nel documento e la trasferisce in formato leggibile su un apposito supporto idoneo a soddisfare la richiesta del giudice;
d) il Notaio redige processo verbale di quanto avvenuto in sua presenza;
e) il Notaio fa avere una copia del verbale delle operazioni realizzate.

14 Violazione dei dati

Ogni evento che implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni e dei dati è gestito dalla Banca secondo specifiche Linee Guida, Policy e Regolamenti, in ottemperanza alla normativa esterna vigente, con particolare riferimento a:

- Banca d'Italia, Circolare n°263 del 27 dicembre 2006 (15° aggiornamento del 2 luglio 2013), Titolo V, capitolo 8, Sezione IV, "La gestione della sicurezza informatica", La sicurezza delle informazioni e delle risorse ICT;
- Decreto Legislativo 30 giugno 2003, n.196 - "Codice in materia di protezione dei dati personali" e i provvedimenti emanati dall'Autorità Garante per la protezione dei dati personali;
- Banca Centrale Europea, Recommendations for the Security of Internet Payments, Gennaio 2013;
- Ispirata allo Standard ISO/IEC 27001 del 2013 (Annex A, A.16 Information security incident management);
- Provvedimento n. 513 del "Garante per la protezione dei dati personali" del 12 novembre 2014;
- Linee Guida EBA emanate il 19 Dicembre 2014, in vigore dal 1° Agosto 2015.

15 Conservazione dei documenti

La conservazione dei documenti informatici sottoscritti con Firma Elettronica Avanzata (FEA) viene svolta in modalità digitale.
La normativa vigente prevede l'obbligatorietà della conservazione a norma di legge dei documenti firmati con Firma Elettronica Avanzata (FEA).
La Banca ha sottoscritto un contratto con Telecom Italia che prevede l'esternalizzazione del Servizio di conservazione sostitutiva con sub-appalto alla società Doxee Spa. Tale sub-esternalizzazione è stata gestita secondo la normativa vigente al momento della sottoscrizione. La società Doxee Spa è un Conservatore che svolge le proprie attività secondo le regole fissate dal D.P.C.M. 3.12.2013.
La società Doxee Spa provvede alla conservazione a norma di legge dei documenti firmati con firma elettronica avanzata, adottando e garantendo ogni misura necessaria per la sicurezza fisica e logica del sistema preposto al processo di conservazione, compresa la continuità operativa e il Disaster Recovery.

16 Copertura rischi

In conformità alla normativa vigente, al fine di proteggere i titolari della Firma Elettronica Avanzata (FEA) ed i terzi da eventuali danni cagionati da inadeguate soluzioni tecniche, la Banca ha attivato specifica copertura assicurativa per la responsabilità civile con la Società Generali Italia Spa (rif. Appendice n. 348758542 – Polizza n. 338758586).

17 Anomalie e Gestione Straordinaria

La soluzione di Firma Elettronica Avanzata (FEA) descritta è stata progettata al fine di garantire il massimo livello di protezione e sicurezza delle informazioni. Tutte le componenti tecnologiche coinvolte, sono strettamente necessarie per il completamento del processo di Firma Elettronica Avanzata (FEA). La mancanza di connettività dati, l'indisponibilità del servizi, il malfunzionamento delle applicazioni Client o Server, di fatto rendono il processo compromesso e quindi si rende necessaria l'apposizione della firma da parte del cliente sui tradizionali moduli cartacei.

18 Variazione della modalità di messa a disposizione e Revoca del Servizio FEA

La variazione della modalità di messa a disposizione della copia di pertinenza del cliente (in forma cartacea, su Smart, attraverso invio a indirizzo e-mail) o la revoca del servizio può avvenire da parte del Firmatario in qualsiasi momento, a titolo gratuito. La variazione o la revoca non ha effetto sui documenti già sottoscritti antecedentemente alla data di variazione o revoca.

Il processo di variazione della modalità di messa a disposizione dei documenti o revoca dell'adesione è subordinato ai seguenti passi operativi:

- **Identificazione del Firmatario**: l'Operatore Banca ha la responsabilità di identificare in modo certo il Firmatario. L'identificazione avviene mediante esibizione di un documento di identità in corso di validità con riconoscimento "de visu". Per la sola variazione della modalità di messa a disposizione il documento di identità esibito, dopo le verifiche necessarie, viene acquisito mediante dispositivo scanner al fine di essere conservato assieme al modulo di variazione a norma di legge, mentre nessun documento di identità è richiesto in caso di revoca del Servizio FEA.
- **In caso di Variazione della modalità di messa a disposizione della copia Cliente**: l'operatore Banca richiede al Cliente la nuova modalità con cui intende ricevere copia della documentazione da lui sottoscritta, scelta fra quelle tempo per tempo messe a disposizione dalla Banca (Smart/CBI, e-mail, cartacea e, di prossima attivazione, e-mail PEC) e la registra nell'applicativo Banca;
- **In caso di Revoca del Servizio FEA** : l'Operatore Banca richiede al Cliente conferma sulla sua volontà di revocare il Servizio e la registra nell'applicativo Banca.
- **Sottoscrizione della Variazione/Revoca**: una volta identificato il Firmatario e scelta la variazione/revoca del Servizio e raccolta (per la sola variazione) la copia elettronica del documento di identità, l'applicativo Banca genera il modulo di Variazione/Revoca del Servizio FEA ed attiva il processo di firma. Viene visualizzata l'anteprima del documento sul monitor dell'Operatore Banca, che con apposito comando trasferisce il controllo della Signature Pad al Firmatario, così che questi possa:
  - prendere visione del modulo scorrendo le pagine sullo schermo usando l'apposito pennino;
  - procedere alla sottoscrizione, toccando con l'apposito pennino lo schermo in corrispondenza del campo firma del modulo. Si aprirà un "box di firma" dove dovrà apporre la propria firma e confermarla (o ripeterla o annullarla) per terminare l'attività sul Signature Pad.

  Per consentire il controllo del documento firmato, questo viene visualizzato sul monitor dell'Operatore Banca, che dovrà quindi cliccare su "conferma (oppure su "ripeti firma" per far ripetere la firma al Cliente, oppure su "annulla" per ritornare nella mappa principale dell'applicativo di adesione).
  In automatico si aprirà una finestra di riepilogo contenente:
  - l'informazione della modalità scelta dal cliente (Smart/CBI, e-mail, cartacea e, di prossima attivazione, e-mail PEC) l'immagine del modulo di variazione/revoca firmato dal Cliente e, in forma digitale, dalla Banca;
  - Il pulsante "Stampa", per stampare una copia cartacea, indipendentemente dalla modalità scelta dal cliente;
  - Il pulsante "Chiudi", che l'Operatore Banca dovrà cliccare per concludere il processo di Firma FEA allo sportello.

La copia "Banca" del modulo, unitamente ai dati grafometrici della firma del Cliente, non viene stampata ma memorizzata elettronicamente ed inviata in conservazione secondo la normativa vigente. Il documento viene conservato elettronicamente a norma di legge nella sua forma di PDF/A dal Responsabile della Conservazione.
La copia "Cliente" viene invece messa a disposizione secondo la scelta da questi effettuata.
Su richiesta del cliente, indipendentemente dalla scelta effettuata, l'Operatore Banca può stampare il documento in forma cartacea al termine dell'operazione effettuata.
Copia cartacea del documento può essere richiesta dal Cliente in ogni momento presso qualsiasi dipendenza della Banca a titolo gratuito.