Deutsche Bank

Firma Grafometrica - db La Mia Firma

Manuale Operativo sui sistemi hardware e software a supporto della gestione del processo di Firma Grafometrica e della relativa documentazione prodotta

Deutsche Bank S.p.A. - Sede Sociale e Direzione Generale: Piazza del Calendario, 3 - 20126 Milano
Tel.: 02.4024.1 - Indirizzo Telegrafico: CENTMERIT Milano - www.db.com/italia - Indirizzo S.W.I.F.T.: DEUT IT MM - Telex: 311350 BAIDIR I - Telefax: S.T.M.: 02.4024.2636 Capitale Sociale Euro 412.153.993,80 - Numero iscrizione al Registro delle Imprese di Milano, Codice Fiscale e Partita IVA: 01340740156.
Aderente al Fondo Interbancario di Tutela dei Depositi - Aderente al Fondo Nazionale di Garanzia ex art. 59 decreto legislativo n. 58/1998 - Iscritta all'Albo delle Banche e Capogruppo del Gruppo Deutsche Bank iscritto all'Albo dei Gruppi Bancari - Soggetta all'attività di direzione e coordinamento della Deutsche Bank AG - Cod. Az. 3104.7

INDICE

1. CONTESTO DI RIFERIMENTO

Con l'obiettivo di migliorare la qualità e la sicurezza dei propri servizi, riducendo al contempo i costi economici ed ambientali per l'erogazione degli stessi, Deutsche Bank S.p.A. fornisce alla Clientela un servizio di sottoscrizione della documentazione contrattuale e di quella necessaria per l'esecuzione dei servizi prestati mediante modalità elettroniche.

Tale servizio prevede l'utilizzo di dati biometrici comportamentali rilevati all'atto della sottoscrizione che costituiranno gli elementi della firma del Cliente secondo le modalità previste per la cosiddetta "Firma Elettronica Avanzata".

Al fine di perseguire l'obiettivo presentato, esso è declinato nei suoi elementi operativi:

- Garantire l'attivazione del servizio e tracciare l'adesione ed il consenso privacy;
- Garantire la generazione di documenti elettronici direttamente dalle procedure aziendali da sottoporre alla firma Cliente;
- Gestire il processo di firma grafometrica della documentazione di riferimento nel rispetto delle regole e policy di sicurezza della banca;
- Gestire i documenti firmati al fine di garantirne la conservazione legale secondo le leggi vigenti e le evoluzioni future;
- Gestire i documenti firmati al fine di garantire l'operatività delle strutture di back-office bancarie.

2. OBIETTIVO DEL PRESENTE DOCUMENTO

Obiettivo del presente documento è descrivere la soluzione tecnica che supporti la gestione del processo di Firma Grafometrica in filiale ed in "offerta fuori sede", nonché la gestione della documentazione così firmata.

Le presenti indicazioni sono redatte anche ai sensi di quanto previsto dal "Provvedimento generale prescrittivo in tema di biometria" n. 513 del 12.11.2014 emanato dal Garante per la Protezione dei Dati Personali (di seguito il "**Provvedimento**").

Nell'esecuzione del servizio, Deutsche Bank tratta i dati personali dei clienti (dati biometrici) in conformità alla normativa sulla protezione dei dati personali (il d.lgs. n. 196/2003 e Provvedimento). In particolare, con riferimento ai principi di:

- Necessità del trattamento: il trattamento dei dati biometrici è indispensabile ai fini dell'erogazione del servizio nel rispetto della normativa bancaria e finanziaria di riferimento nonché delle previsioni del d.lgs. n. 82/2005 (il c.d. "Codice dell'Amministrazione Digitale");
- Liceità e correttezza del trattamento: i dati sono prelevati e trattati in conformità al d.lgs. n. 196/2003 ed al Provvedimento;
- Finalità del trattamento: i dati sono prelevati e trattati unicamente ai fini dell'erogazione del servizio agli interessati, i quali sono adeguatamente informati degli scopi, delle modalità e delle garanzie del trattamento;
- Proporzionalità del trattamento: i dati prelevati e trattati sono solo i dati biometrici strettamente necessari ed indispensabili all'erogazione del servizio stesso;
- Corretta conservazione dei dati: i dati sono conservati in maniera tale da poter verificare la correttezza della firma dell'interessato nel caso in cui venga promosso un contezioso davanti l'autorità giudiziaria e la loro conservazione è mantenuta solo per il tempo strettamente necessario per l'erogazione del servizio e in conformità a quanto previsto dalle norme di legge in materia di conservazione della documentazione;

- Accessibilità dei dati: l'interessato ha sempre la possibilità di accedere ai propri dati personali.

Deutsche Bank si riserva di modificare e aggiornare il presente documento anche alla luce della imminente applicazione del Regolamento UE n. 679/2016 in materia di protezione di dati personali (cfr. art. 99, co. 2 del Regolamento).
In tal senso, la Banca sta già svolgendo un'analisi di impatto della nuova normativa e tale documento verrà rivisto e integrato per rendere le procedure e le soluzioni relative ai trattamenti qui descritti conformi alle nuove previsioni del suddetto Regolamento entro il termine della sua applicazione (25 maggio 2018).
In generale, la Banca provvederà a revisionare e ad aggiornare il presente documento almeno una volta all'anno.

3. TECNOLOGIA ABILITANTE SIGNOTEC

La soluzione implementata da Deutsche Bank per la gestione del processo di firma grafometrica si basa sulla tecnologia messa a disposizione dalla società Signotec GmBH, tecnologia selezionata anche presso la capogruppo Deutsche Bank AG in Germania in quanto pienamente aderente alle policy di sicurezza interne al Gruppo Deutsche Bank.

La soluzione tecnologica Signotec si compone dei seguenti elementi:
- Hardware per la rilevazione dei dati biometrici (di seguito "***Signpad***");
- Software che controlla direttamente il **Signpad** e che consente la gestione del processo di firma

In ambiente iOS si compone invece dei seguenti elementi:
- Hardware di supporto alla rilevazione dei dati biometrici (di seguito "**iPad**");
- Software: libreria "**Signotec libSignoPDFSigner**" che consente la gestione del processo di firma

3.1 CARATTERISTICHE TECNICHE DELL'HARDWARE SIGNOTEC

Sono di seguito riportate le principali caratteristiche distintive dell'Hardware Signotec:

Schermo per visualizzazione documenti
- Il **Signpad** presenta uno schermo TFT per la visualizzazione del documento da firmare e consente di rilevare i dati biometrici mediante l'utilizzo di un pennino;
- La visualizzazione di un documento sul **Signpad** è interamente governata dal relativo Software che invia al device le singole immagini del documento da firmare (non si tratta pertanto di una visualizzazione tramite "estensione dello schermo") consentendo pertanto di mantenere distinto quanto un Operatore vede a video del proprio terminale e quanto è visualizzato sul **Signpad**;
- Le dimensioni del video, disponibili sui differenti modelli di Singpad sono:
  - 5" (denominato "OmegaPad"): tale modello potrà essere utilizzato solo presso gli sportelli che presenteranno esclusiva operatività di cassa per la firma di distinte e contabili
  - 10" (denominato "DeltaPad"): tale modello, appena reso disponibile, potrà essere utilizzato presso tutti gli sportelli che presenteranno operatività sia di cassa che di apertura contratti

Tecnologia per la rilevazione dei dati biometrici
- La rilevazione dei dati biometrici da parte del **Signpad** è condotta mediante la tecnologia di Risonanza Magnetica (ERT: Electromagnetic Resonance Technology)
- La firma è condotta mediante un apposito pennino passivo (non presenza di batterie)
- La pressione del tratto è rilevabile su 1024 livelli
- La frequenza di rilevazione del campione: 280 rilevazioni al secondo

- Le caratteristiche comportamentali a contenuto biometrico rilevate sono: le coordinate X (posizionamento orizzontale del pennino) e Y (posizionamento verticale del pennino), il tempo di firma e la pressione del pennino sullo schermo, sulla base delle quali vengono calcolati, in caso di necessità di analisi, dal Software di decriptazione la velocità lineare, l'accelerazione lineare, la velocità radiale, l'angolo di inclinazione ed i punti di discontinuità
- Unitamente ai precedenti dati sono anche tracciate le seguenti informazioni: numero seriale, origine della chiave di firma, opzioni del device, versione *firmware*, risoluzione del sensore, risoluzione LCD, livello di *adjustment* del sensore, rotazione del display, risoluzione della pressione, soglie applicate, frequenza rilevazione campione, *time-stamp*, algoritmo usato per la generazione *hash*.

Sicurezza per le operazioni di firma

- I dati biometrici sono rilevati tramite il **Signpad**.
- La cifratura dei dati biometrici è condotta direttamente all'interno del dispositivo mediante apposito chip crittografico (non si tratta quindi di un emulazione Software) che supporta i seguenti algoritmi per la generazione dell'hash: SHA-1, SHA-256 and SHA-512 e RSA 2048 per la cifratura.
- La cifratura dei dati biometrici avviene a pacchetti durante il processo di firma all'interno del dispositivo in modo che non possano mai risiedere in chiaro neanche nella memoria del **Signpad**; unitamente ai dati biometrici viene cifrato anche il numero seriale del dispositivo e le ulteriori caratteristiche rilevate I dati cifrati sono, al termine del processo di firma, comunicati all'applet che provvede ad inserirli all'interno del documento di riferimento *pdf*.
- La cifratura dei dati biometrici è condotta utilizzando un certificato digitale X.509 precaricato su ciascun **Signpad** che è fornito direttamente dalla Banca. Ogni **Signpad** presenterà un proprio certificato che potrà essere certificato da una Certification Authority.
- Gli schemi supportati sono RSA PKCS # 1 v1.5 (con o senza hash OID), PKCS # 1 v2.
- Il documento viene quindi firmato all'interno del **Signpad**, e non nell'ambiente di esecuzione dell'Applicazione ospitante (i.e. il PC).
- La firma è condotta secondo gli standard Adobe *pdf* in modo da poter essere verificata utilizzando un qualunque Software compatibile presente sul mercato.

Sicurezza per la gestione dei certificati RSA

- I certificati X.509 alla base del processo di firma sono forniti direttamente dalla Banca e precaricati su ciascun **Signpad**
- Al fine di garantire la sicurezza di tali certificati ed un loro processo di aggiornamento sicuro nel tempo sono previste funzionalità dedicate protette da password

	Factory Default	With device password	With key lock
Read private signing key	No	No	No
Read public signing key	Yes	Yes	Yes
Read certificate signing request	Yes	Yes	Yes
Generate signing key pair	Yes	Password needed	No
Store signing key pair	Yes	Password needed	No
Read public encryption key	No	No	No
Read public encryption key description	Yes	Yes	Yes
Store public encryption key	Yes	Password needed	No
Set / change / delete device password	Yes	Password needed	No
Set permanent key lock	Yes	Yes	No

3.2 CARATTERISTICHE TECNICHE DEL SOFTWARE SIGNOTEC

Sono di seguito riportate le principali caratteristiche distintive del Software Signotec:

- Rappresenta l'unica modalità di interfacciamento nei confronti del **Signpad** e ne consente il pieno controllo mediante comandi a video (da parte dell'Operatore di sportello) e parametri di impostazione (da parte di applicazioni che richiamano l'applet).
- È costituito da una Applet Java in modo da poter essere richiamato all'interno di specifiche applicazioni banca e potersi interfacciare con le medesime, per la gestione della documentazione da firmare.
- Costituisce il front-end dell'Operatore di sportello per gestire il processo di visualizzazione e firma di uno specifico documento presso il **Signpad** collegato in modalità end to end.
- Riceve dal **Signpad** i dati biometrici già criptati e provvede ad incorporarli all'interno del documento; una volta incorporati vengono cancellati e sovrascritti dalla memoria (ram) del computer, non risultando conseguentemente visualizzabili né dagli Operatori né da altri operatori interni alla Banca o da parte di altri operatori coinvolti nella gestione documentale
- Il Software Signotec è certificato dall'ente di certificazione TűV [*Technischer Überwachungs-Verein*]
- La libreria iOS libSignoPDFSigner, similmente all'Applet Java per la webapp, gestisce il processo di visualizzazione e firma e incorpora la firma all'interno del documento.

3.3 CARATTERISTICHE TECNICHE DELLA CONNESSIONE SIGNPAD - THIN CLIENT

Le caratteristiche del **Signpad** e le modalità di connessione previste garantiscono la non accessibilità dei dati né durante il processo di firma né durante la permanenza dei dati sui sistemi della Banca.

- I **Signpad** non possiedono un sistema operativo atto all'installazione di Software ma interagiscono esclusivamente con l'Applet Signotec.
- I **Signpad** sono collegati ai *computer* o ai *thin client* mediante collegamento intranet in modalità criptata.
- La presenza all'interno del **Signpad** di un certificato proprietario della Banca su cui basare l'algoritmo di cifratura presupporrebbe che, per intercettare e decifrare i dati biometrici, la corrispondete chiave privata venisse trafugata.
- I *computer* o i *thin client* distribuiti presso le filiali banca presentano livelli di sicurezza in linea con le policy Deutsche Bank e presentano, ad esempio, tutte le porte USB disabilitate nelle funzionalità di trasferimento files.

4. DESCRIZIONE DELL'INFRASTRUTTURA DI RIFERIMENTO

La soluzione implementata da DB per supportare il processo di firma si basa sull'applicazione residente sui sistemi centrali della Banca ed è accessibile solo all'interno della rete informatica di DB dai singoli computer o thin client.

Il Signpad è connesso al computer o al thin client dell'Operatore di sportello, mediante collegamento intranet in modalità cifrata: l'eventuale assenza di una connettività interna (network) comporta il blocco sia della rilevazione dei dati biometrici da parte del **Signpad** che di tutte le funzionalità dell'applicativo di firma.

A livello tecnologico sono di seguito riportate le principali tecnologie adottate:

- DBMS: Oracle
- Middleware: SuSe Linux 11 SP2 on VHS-L
- Enterprise Service Bus: Apache ServiceMix
- Workflow-Engine: Apache Camel

5. DESCRIZIONE DELL'APPLICATIVO A SUPPORTO DEL PROCESSO DI FIRMA GRAFOMETRICA (IN FILIALE)

La soluzione implementata da *Deutsche Bank* per supportare il processo di firma grafometrica si basa su una applicazione dedicata sviluppata dal fornitore InfoCert basata su prodotti proprietari e su tecnologia biometrica Signotec. Nello specifico:

- Il prodotto proprietario InfoCert ("LegalBus") ha l'obiettivo di gestire sia il processo di firma che le interfacce in input della documentazione prodotta in automatico dai sistemi a monte ed in output per l'invio della documentazione firmata ai sistemi documentali identificati;
- L'applicazione custom InfoCert ("Applicativo di Firma Grafometrica") ha l'obiettivo di gestire la user experience dell'Operatore prima e durante le operazioni di firma;
- Il Software Signotec, interfacciato all'interno dell'Applicativo di Firma Grafometrica, ha l'obiettivo di gestire l'interazione con il **Signpad** durante l'operatività di firma.

Nei successivi paragrafi è riportata una descrizione tecnico-funzionale dell'applicativo con l'obiettivo di presentarne sinteticamente l'operatività e di evidenziare gli aspetti di sicurezza nella gestione del processo di firma.

5.1 ACCESSO ALL'APPLICATIVO DA PARTE DEGLI UTENTI DI SPORTELLO E TRACCIABILITA'

- L'utente viene accreditato sull'applicazione di firma mediante servizi di *Single Sign On* presenti a livello Banca in base alle credenziali inserite direttamente sulla macchina.
- L'utente, in base al ruolo ricoperto, è assegnato ad un proprio profilo di operatività al fine di garantire una corretta profilazione delle funzionalità messe a disposizione dall'applicativo.
- L'applicazione di firma possiede un proprio Log con cui tracciare le utenze e gli accessi
  - L'applicazione LegalBus è composta in sintesi da un insieme di nodi funzionali collegati tra di loro all'interno di una pipeline di processo. Le informazioni oggetto di processamento vengono scambiate con l'esterno tramite opportuni componenti di integrazione.
  - Il sistema di log impostato su LegalBus si occupa di mantenere l'attività del sistema durante l'intera transazione collegata al processo.
- Vengono di seguito riportate le informazioni a supporto del logging in termini di contesto e di flessibilità di configurazione:
  - Logging: contesto
    - Le informazioni oggetto di log sono sostanzialmente di due tipi:
      - Dati relativi all'instradamento: inserimento/uscita da un processo, input/output dal sistema LegalBus verso ambienti applicativi esterni.
      - Informazioni sulla gestione dei dati ad opera dei nodi applicativi; tipicamente consistono in trasformazioni del contenuto informativo del dato in transito sia in termini di tracciato binario che di singolo metadato.
  - Logging: configurazione
    - Il sistema di log è a 5 livelli: DEBUG, INFO, WARNING, ERROR, FATAL; ciascuna informazione inserita in una istruzione di log (logger) può essere associata ad un differente livello.
    - Tale classificazione definisce l'effettiva scrittura o meno nella coda di output (appender) secondo un criterio gerarchico basato sulla configurazione del server.
    - L'esito del log, nella configurazione di default di LegalBus, è impostato in parallelo su due output: filesystem e console.
    - I file di log sono generati, su filesystem locale o remoto, con cadenza giornaliera.

5.2 PRINCIPALI FUNZIONALITÀ APPLICATIVE DISPONIBILI A LIVELLO UTENTE

Sono di seguito elencate le principali funzionalità previste a livello applicativo:

- Ricerca pratiche
  - Ricerca e visualizzazione dell'elenco pratiche da firmare o in firma gestite dall'Operatore loggato
  - Ricerca e visualizzazione dell'elenco pratiche da firmare o in firma afferenti allo sportello di appartenenza
  - Ricerca e visualizzazione dell'elenco pratiche che risultano già firmate

- Visualizzazione dettagli pratica
  - Visualizzazione delle informazioni generali afferenti una pratica
  - Visualizzazione del dettaglio ordini / prodotti contenuti all'interno di una pratica
  - Visualizzazione del dettaglio documenti relativi ai singoli prodotti
  - Visualizzazione della documentazione generale della pratica (documenti comuni ai prodotti)

- Acquisizione documentazione
  - Acquisizione di documentazione generata automaticamente da procedure esterne
  - Acquisizione manuale di documentazione mediante utilizzo dello scanner installato presso gli sportelli
  - Acquisizione manuale di documentazione mediante upload di file elettronici
  - Classificazione della documentazione acquisita

- Firma della documentazione
  - Attivazione del processo di firma mediante applet Signotec (vedere paragrafo 5.4)

- Cancellazione di documenti / pratiche (viene applicato il principio dei quattro occhi, ovvero l'Operatore propone la cancellazione ed il responsabile di filiale - o suo facente funzione - conferma)
  - Cancellazione di un documento non ancora firmato
  - Cancellazione di un documento con firme grafometriche già apposte
  - Cancellazione di una pratica o di un ordine non ancora elaborati
  - Cancellazione di una pratica o di un ordine con firme grafometriche già apposte

5.3 ACQUISIZIONE DEI DOCUMENTI IN INPUT

L'acquisizione dei documenti in input può avvenire secondo le seguenti modalità:

- Acquisizione automatica
  - La documentazione (i.e. modulistica contrattuale) viene generata in automatico da procedure esterne (i.e. Applicativo di Sportello)
  - Una nuova pratica / sessione di firma può essere generata solo dall'acquisizione di documentazione automatica da parte di un sistema esterno interfacciato.
  - Le procedure esterne si interfacciano con l'applicazione di Firma Grafometrica segnalando la presenza di specifica documentazione e comunicano, in modalità automatica e trasparente all'utente, tutte le informazioni per la gestione operativa del processo di firma (i.e. tipologia documenti, codice della pratica e dei prodotti componenti, dettaglio degli utenti che devono operativamente apporre la loro firma)
  - Nello specifico, l'informazione sugli utenti che devono operativamente firmare la documentazione recepita in firma è reperita all'interno delle procedure di sportello in modo da essere coerente con l'operatività di riconoscimento della Clientela e di verifica dei poteri

di firma per l'operazione in corso. L'Operatore di sportello è pertanto guidato a livello applicativo nel far firmare una pratica a coinvolgere solo gli utenti aventi diritto ed aventi corretto potere di firma su di essa.

- Acquisizione manuale mediante utilizzo diretto dello scanner
  - Qualora sia necessario integrare la documentazione acquisita in automatico con ulteriori documenti cartacei (i.e. allegati contrattuali forniti dal Cliente, copia documenti d'identità) è possibile effettuare una scansione degli stessi tramite lo scanner disponibile ai singoli sportelli.
  - Il documento, una volta scannerizzato, è incluso all'interno della pratica in lavorazione e potrà essere inviato o meno alla firma in base alle necessità dettate dal documento

- Acquisizione manuale mediante upload di file
  - Qualora sia necessario integrare la documentazione acquisita in automatico con ulteriori documenti in formato elettronico (i.e. modulistica compilata manualmente dallo sportellista) è possibile allegarli alla pratica
  - Il documento, una volta caricato all'interno della pratica, è classificato dall'Operatore e può essere inviato o meno alla firma.

5.4 ESECUZIONE OPERATIVA DEL PROCESSO DI FIRMA

L'esecuzione operativa del processo di firma è interamente gestita dal Software Signotec integrato all'interno dell'applicativo di Firma Grafometrica che consente un interfacciamento diretto con il **Signpad** Signotec.

Il Software Signotec supporta le seguenti funzioni:

- Interfacciamento diretto con altri applicativi in input / output
  - Acquisizione in input della documentazione in formato *pdf* da altri sistemi fonte (nello specifico dall'Applicativo di Firma Grafometrica) unitamente ai parametri di firma che devono essere applicati ai singoli documenti
  - Restituzione in output dei documenti in formato *pdf* contenenti già le firme in modalità cifrata
  - Interfacciamento diretto del **Signpad** per la gestione dell'interattività con l'utente finale
- Visualizzazione sul video dell'Operatore dei documenti da firmare
  - Visualizzazione dei documenti prima del processo di firma per una verifica di leggibilità
  - Visualizzazione del documento durante il processo di firma per una verifica sull'operatività dell'utente che sta operando direttamente sul **Signpad**
- Identificazione automatica dei punti firma
  - Mediante coordinate predefinite
  - Mediante identificazione di un testo predefinito ("ancora")
- Aggiunta di ulteriori punti firma
  - Possibilità da parte dell'Operatore di definire con il mouse ulteriori punti firma ad hoc in base alle esigenze puntuali
- Invio a firma di un documento mediante **Signpad** Signotec
  - Gestione della visualizzazione del documento sul **Signpad**
  - Gestione dei pulsanti per l'operatività utente visualizzati sul **Signpad**
- Processo di acquisizione firme Cliente per i campi firma previsti (dettaglio successivo)
  - Esecuzione della cifratura dei dati all'interno del **Signpad**
  - Invio dei dati cifrati al Software Signotec
- Verifica automatica della presenza delle firme apposte

E' di seguito riportata la sequenza degli step operativi previsti per l'acquisizione delle firme:

- Il Software Signotec invia al **Signpad** l'hash (Hash1 sha256) del documento
- Durante il rilevamento dei dati biometrici, un secondo hash (Hash 2 sha256) viene generato nel **Signpad** includendo i dati biometrici e le informazioni sul *device*
- Al termine dell'apposizione della firma, i due hash sono combinati e firmati all'interno del **Signpad** con la chiave privata ed inviati al Software Signotec che li include nel file *.pdf*. Informazioni sulla chiave pubblica sono inviate al Software Signotec per consentire di verificare che la firma sia associata al documento corretto.
- I dati biometrici di firma, unitamente ad altri dati tecnici sono criptati all'interno del **Signpad** unitamente all'Hash1, il numero seriale del **Signpad** ed il *time-stamp*. Sono anch'essi inviati al Software Signotec che li include nel file *.pdf*. Tale accorgimento garantisce che i dati biometrici siano associati univocamente al documento originario
- Al termine delle procedure sulle singole firme effettuate, il Software Signotec calcola un terzo hash (Hash 3 sha1) che contiene tutti i dati precedentemente collezionati al fine di essere firmato sul **Signpad** con la chiave privata. Tale step garantisce la compatibilità con lo standard di firma Acrobat Digital Signature. L'hash ricevuto (Hash 3) viene firmato con la chiave privata sul **Signpad** ed inviato al Software Signotec
- Il Software Signotec include nel file *pdf* l'hash documento completo unitamente alla chiave pubblica precedentemente acquisita.

5.5 CHIUSURA DEL DOCUMENTO MEDIANTE FIRMA DIGITALE (C.D. "MASSIVA") DELLA BANCA

Dopo la conferma dell'apposizione dell'ultima firma prevista, il documento viene chiuso mediante firma digitale ("massiva") della Banca i cui certificati sono ospitati in un HSM presso il data-center Banca. I certificati sono della Banca ed emessi sotto la responsabilità di InfoCert che agisce in qualità di Certification Autorithy.

L'apposizione della firma digitale ("massiva") della Banca è tracciata anche visivamente a livello di singolo documento mediante inserimento di apposite diciture che riportino l'informazione sulla presenza di una firma digitale, della data/ora della firma e dell'eventuale Operatore che ha seguito il processo di firma (firma *.pdf* "visibile").

5.6 INVIO DEL DOCUMENTO AGLI ARCHIVI DOCUMENTALI

Il documento informatico sottoscritto e chiuso tramite firma digitale ("massiva") della Banca viene inviato tramite canali sicuri a:

- Il "Sistema documentale interno di Deutsche Bank S.p.A" gestito da Microdata per consentirne la visualizzazione ai fini operativi da parte della Banca:
  - A seguito di un processo di "flattering" (cancellazione dei dati biometrici), la documentazione inviata presso tale sistema non contiene al suo interno i Dati Biometrici del Cliente ma la firma è visibile solo sottoforma di tratto grafico;
  - La documentazione è accessibile alle strutture operative della banca per consentire l'erogazione del servizio / prodotto e per eventuale attività di assistenza e controllo.

- Il "Sistema di gestione documentale per la consultazione della documentazione da parte della Clientela" gestito da Microdata:
  - La documentazione inviata presso tale sistema non contiene al suo interno i Dati Biometrici del Cliente;

- La consultazione della documentazione da parte della Clientela avviene tramite il servizio db Interactive nell'area MyDocuments ovvero fruibile all'interno dei servizi internet dbDocumentiOnline, nonché db Interactive (internet banking) per i clienti che hanno attivato tale servizio.

o l'archivio di conservazione a norma gestito da InfoCert per la relativa conservazione:
  - La documentazione inviata presso tale sistema contiene al suo interno, in modalità cifrata, i Dati Biometrici del Cliente e non è accessibile alla Clientela ma solamente ad utenti designati della Banca.

6. IL PROCESSO OPERATIVO DI FIRMA ELETTRONICA AVANZATA (IN FILIALE)

Viene di seguito riportato il processo operativo di firma nella sua interezza.

6.1 IDENTIFICAZIONE DEL CLIENTE

1. Qualora un Cliente si presenti allo sportello di una filiale abilitata ad operare in modalità grafometrica, il dipendente presso la filiale della Banca (di seguito, "Operatore") identifica il Cliente.

6.2 REGISTRAZIONE ADESIONE AL SERVIZIO DI FIRMA ELETTRONICA AVANZATA

2. Qualora il Cliente richieda di avvalersi del Servizio di FEA, l'Operatore lo identifica e, nel caso si tratti di un nuovo Cliente, lo censisce all'interno delle Procedura di Sportello.
3. Al fine di consentire la sottoscrizione dei documenti tramite FEA, l'Operatore accede alla specifica funzionalità internamente alla Procedura di Sportello in modo da stampare i moduli previsti.
4. Successivamente alla consegna al Cliente dell'informativa Privacy, il Cliente sottoscrive, su supporto cartaceo, sia il consenso al trattamento dei dati biometrici da parte della Banca, sia il contratto per l'utilizzo del Servizio di FEA. Il consenso del Cliente è registrato all'interno della Procedura di Sportello mediante un'apposita transazione.

6.3 OPERATIVITÀ SUL SISTEMA DI SPORTELLO

5. L'Operatore, in base alle necessità operative del Cliente, esegue le transazioni richieste all'interno della Procedura di Sportello.
6. Qualora si richieda la stampa di un modulo o di un documento a firma del Cliente, la Procedura di Sportello verifica che il Cliente o i clienti (nel caso di cointestazioni o vincoli operativi registrati nel Libro Firma) abbia/no aderito al servizio di FEA.
7. Solo se tutti gli aventi diritto di firma hanno aderito al servizio, la Procedura di Sportello propone l'invio del modulo al sistema di Firma Grafometrica mantenendo l'opzione, su volontà del Cliente, di proseguire l'operatività mediante stampa cartacea:
   - Qualora sia scelta l'opzione di stampa cartacea, il documento viene inviato alle stampanti per il processo standard.
   - Qualora sia scelta l'opzione di Firma Grafometrica, la Procedura di Sportello notifica al sistema di Firma Grafometrica la presenza di un documento da firmare.
8. All'interno della stessa operatività nella Procedura di Sportello è possibile inviare al sistema di Firma Grafometrica più documenti in modo da consentire un unico processo di firma.

6.4 OPERATIVITÀ SULL'APPLICAZIONE DI FIRMA GRAFOMETRICA

9. In caso di scelta della modalità di sottoscrizione da parte del Cliente mediante firma grafometrica, l'Operatore, richiama dal suo *computer* o *thin client* il sistema di firma grafometrica: l'accesso all'applicazione comporta il riconoscimento automatico dell'Operatore in base alle credenziali di SSO dallo stesso fornite in fase di login alla postazione.
10. L'applicazione di firma grafometrica è installata all'interno dei *data center* della Banca e fruibile solo all'interno della rete *intranet* di DB per le risorse aventi profili abilitati.
11. La documentazione oggetto del processo di firma risiede all'interno dell'applicazione di firma grafometrica che ne garantisce l'integrità, la completezza e la sicurezza in base alle *policy* della Banca.
12. L'utente accede all'applicazione di Firma Grafometrica per l'operatività richiesta:
    - Visualizzazione della pratica
    - Verifica della documentazione richiesta
    - Visualizzazione dei documenti acquisiti automaticamente
    - Aggiunta di documenti mediante scansione
    - Aggiunta di documenti mediante upload
    - Avvio dell'operatività di firma
13. Il **Signpad** è connesso al *computer* o al *thin client* dell'Operatore di sportello, mediante collegamento intranet in modalità cifrata: l'eventuale assenza di una connettività interna (network) comporta il blocco sia della rilevazione dei dati biometrici da parte del **Signpad** che di tutte le funzionalità dell'applicativo di firma.
14. Il documento elettronico in formato *.pdf* è inviato al **Signpad** attraverso l'applicazione di Firma Grafometrica su richiesta dell'Operatore affinché lo stesso documento sia pronto per essere firmato dal Cliente. L'Operatore, durante il processo di firma, ha la possibilità di visualizzare il documento presente sul **Signpad** in modo da verificare l'operatività del Cliente.
15. Il Cliente prende visione del documento elettronico ed appone la firma sul **Signpad** il quale acquisisce i Dati Grafometrici contestualmente all'apposizione della firma.
16. Il Cliente ha il controllo esclusivo del processo di firma e dispone delle seguenti funzioni:
    - Visualizzazione integrale del documento in modo da avere cognizione piena di quanto si accinge a sottoscrivere;
    - Avvio dell'inserimento di una firma mediante apposito tasto;
    - Conferma della firma apposta mediante apposito tasto;
    - Cancellazione della firma apposta per riscriverla in caso di errore mediante apposito tasto;
    - Annullamento dell'inserimento della firma mediante un apposito tasto;
    - Annullamento della procedura di firma del documento mediante apposito tasto.
17. Mentre il Cliente appone la firma con il pennino a disposizione, i Dati Grafometrici vengono immediatamente cifrati e progressivamente inviati all'applicazione di Firma Grafometrica.
18. I Dati Grafometrici sono cifrati all'interno del **Signpad** avvalendosi di un *chip* dedicato ed inviati all'Applet Signotec su canale cifrato. L'Applet Signotec recepisce i dati cifrati e li inserisce all'interno del documento in formato *.pdf.*
19. Al termine della procedura di firma da parte del Cliente, sono generate una serie di stringhe *hash* per la successiva verifica dell'integrità della firma in caso di contestazione da parte del Cliente nell'ambito di un contenzioso avanti l'autorità giudiziaria e dei documenti acquisiti in formato elettronico, anch'esse cifrate con la chiave pubblica installata nel dispositivo, con algoritmo RSA.

20. Se i sottoscrittori sono più di uno o sono richieste più firme del medesimo soggetto, il sistema ripeterà le operazioni sopra descritte per ciascuna firma necessaria, eventualmente anche in tempistiche differenti.

6.5 CHIUSURA DEL DOCUMENTO MEDIANTE FIRMA DIGITALE (C.D. "MASSIVA") DELLA BANCA

21. Dopo la conferma dell'apposizione dell'ultima firma prevista, il documento viene chiuso mediante firma digitale ("massiva") della Banca, il cui certificato e relativa chiave privata sono ospitati in un HSM sotto la responsabilità di InfoCert che agisce in qualità di *Certification Autorithy* L'HSM è installato presso il data-center Banca.

6.6 INVIO DEL DOCUMENTO AI SISTEMI DOCUMENTALI

22. Il documento informatico sottoscritto e chiuso tramite firma digitale ("massiva") della Banca viene inviato tramite canali sicuri a:
    - Il "Sistema documentale interno di Deutsche Bank S.p.A" gestito da Microdata per consentirne la visualizzazione ai fini operativi da parte della Banca.
    - Il Sistema documentale per la consultazione della documentazione da parte della Clientela, gestito da Microdata.
    - L'archivio di conservazione a norma gestito da InfoCert.

7. DESCRIZIONE DELL'APPLICATIVO A SUPPORTO DEL PROCESSO DI FIRMA GRAFOMETRICA (OFFERTA FUORI SEDE)

La soluzione implementata da *Deutsche Bank* per supportare il processo di firma grafometrica si basa su una applicazione dedicata sviluppata dal fornitore InfoCert basata su prodotti proprietari e su tecnologia biometrica Signotec. Nello specifico:

- Il prodotto proprietario InfoCert ("LegalBus") ha l'obiettivo di gestire sia il processo di firma che le interfacce in input della documentazione prodotta in automatico dai sistemi a monte ed in output per l'invio della documentazione firmata ai sistemi documentali identificati;
- L'applicazione mobile custom InfoCert ("App di Firma Grafometrica") ha l'obiettivo di gestire la user experience dell'Operatore prima e durante le operazioni di firma;
- Il Software Signotec, interfacciato all'interno dell'App di Firma Grafometrica, ha l'obiettivo di gestire l'interazione con il **tablet** durante l'operatività di firma.

Nei successivi paragrafi è riportata una descrizione tecnico-funzionale dell'applicativo con l'obiettivo di presentarne sinteticamente l'operatività e di evidenziare gli aspetti di sicurezza nella gestione del processo di firma.

7.1 ACCESSO ALL'APP DI FIRMA DA PARTE DEGLI UTENTI FUORI SEDE E TRACCIABILITA'

- L'utente viene accreditato sull'app di firma mediante servizi di *Single Sign On* presenti a livello Banca in base alle credenziali inserite direttamente sul tablet.
- L'utente, in base al ruolo ricoperto, è assegnato ad un proprio profilo di operatività al fine di garantire una corretta profilazione delle funzionalità messe a disposizione dall'app.
- L'app di firma possiede un proprio Log con cui tracciare le utenze e gli accessi

- L'applicazione LegalBus è composta in sintesi da un insieme di nodi funzionali collegati tra di loro all'interno di una pipeline di processo. Le informazioni oggetto di processamento vengono scambiate con l'esterno tramite opportuni componenti di integrazione.
- il sistema di log impostato su LegalBus si occupa di mantenere l'attività del sistema durante l'intera transazione collegata al processo.

o Vengono di seguito riportate le informazioni a supporto del logging in termini di contesto e di flessibilità di configurazione:
  - Logging: contesto
    - Le informazioni oggetto di log sono sostanzialmente di due tipi:
      - Dati relativi all'instradamento: inserimento/uscita da un processo, input/output dal sistema LegalBus verso ambienti applicativi esterni.
      - Informazioni sulla gestione dei dati ad opera dei nodi applicativi; tipicamente consistono in trasformazioni del contenuto informativo del dato in transito sia in termini di tracciato binario che di singolo metadato.
  - Logging: configurazione
    - Il sistema di log è a 5 livelli: DEBUG, INFO, WARNING, ERROR, FATAL; ciascuna informazione inserita in una istruzione di log (logger) può essere associata ad un differente livello.
    - Tale classificazione definisce l'effettiva scrittura o meno nella coda di output (appender) secondo un criterio gerarchico basato sulla configurazione del server.
    - L'esito del log, nella configurazione di default di LegalBus, è impostato in parallelo su due output: filesystem e console.
    - I file di log sono generati, su filesystem locale o remoto, con cadenza giornaliera.

7.2 PRINCIPALI FUNZIONALITÀ APPLICATIVE DISPONIBILI A LIVELLO UTENTE

Sono di seguito elencate le principali funzionalità previste a livello applicativo:

o Ricerca pratiche
  - Ricerca e visualizzazione dell'elenco pratiche da firmare o in firma gestite dall'Operatore loggato
  - Ricerca e visualizzazione dell'elenco pratiche che risultano già firmate

o Visualizzazione dettagli pratica
  - Visualizzazione delle informazioni generali afferenti una pratica
  - Visualizzazione del dettaglio ordini / prodotti contenuti all'interno di una pratica
  - Visualizzazione del dettaglio documenti relativi ai singoli prodotti
  - Visualizzazione della documentazione generale della pratica (documenti comuni ai prodotti)

o Acquisizione documentazione
  - Acquisizione di documentazione generata automaticamente da procedure esterne
  - Acquisizione manuale di documentazione mediante utilizzo della fotocamera del tablet
  - Classificazione della documentazione acquisita

o Firma della documentazione
  - Attivazione del processo di firma mediante applet Signotec (vedere paragrafo 5.4)
  - Attivazione del processo di firma mediante libreria Signotec

- Cancellazione di documenti / pratiche (viene applicato il principio dei quattro occhi, ovvero l'Operatore propone la cancellazione ed il responsabile di filiale – o suo facente funzione - conferma)
  - Cancellazione di un documento non ancora firmato
  - Cancellazione di un documento con firme grafometriche già apposte
  - Cancellazione di una pratica o di un ordine non ancora elaborati
  - Cancellazione di una pratica o di un ordine con firme grafometriche già apposte

7.3 ACQUISIZIONE DEI DOCUMENTI IN INPUT

L'acquisizione dei documenti in input può avvenire secondo le seguenti modalità:

- Acquisizione automatica
  - La documentazione (i.e. modulistica contrattuale) viene generata in automatico da procedure esterne (i.e. Applicativo di Sportello)
  - Una nuova pratica / sessione di firma può essere generata solo dall'acquisizione di documentazione automatica da parte di un sistema esterno interfacciato.
  - Le procedure esterne si interfacciano con l'applicazione di Firma Grafometrica segnalando la presenza di specifica documentazione e comunicano, in modalità automatica e trasparente all'utente, tutte le informazioni per la gestione operativa del processo di firma (i.e. tipologia documenti, codice della pratica e dei prodotti componenti, dettaglio degli utenti che devono operativamente apporre la loro firma)
  - Nello specifico, l'informazione sugli utenti che devono operativamente firmare la documentazione recepita in firma è reperita all'interno delle procedure di sportello in modo da essere coerente con l'operatività di riconoscimento della Clientela e di verifica dei poteri di firma per l'operazione in corso. L'Operatore di sportello è pertanto guidato a livello applicativo nel far firmare una pratica a coinvolgere solo gli utenti aventi diritto ed aventi corretto potere di firma su di essa.

- Acquisizione manuale mediante utilizzo della fotocamera del tablet
  - Qualora sia necessario integrare la documentazione acquisita in automatico con ulteriori documenti cartacei (i.e. allegati contrattuali forniti dal Cliente, copia documenti d'identità) è possibile effettuare una fotografia degli stessi tramite la fotocamera disponibile sul tablet
  - Il documento, una volta fotografato e trasformato nel formato .pdf, è incluso all'interno della pratica in lavorazione

7.4 ESECUZIONE OPERATIVA DEL PROCESSO DI FIRMA

L'esecuzione operativa del processo di firma è interamente gestita dal Software Signotec integrato all'interno dell'applicativo di Firma Grafometrica che consente un interfacciamento diretto con il **Signpad** Signotec o l'iPad

Il Software Signotec supporta le seguenti funzioni:

- Interfacciamento diretto con altri applicativi in input / output
  - Acquisizione in input della documentazione in formato *pdf* da altri sistemi fonte (nello specifico dall'Applicativo di Firma Grafometrica) unitamente ai parametri di firma che devono essere applicati ai singoli documenti
  - Restituzione in output dei documenti in formato *pdf* contenenti già le firme in modalità cifrata
  - Interfacciamento diretto del **Signpad** o iPad per la gestione dell'interattività con l'utente finale
- Visualizzazione sul video dell'Operatore dei documenti da firmare
  - Visualizzazione dei documenti prima del processo di firma per una verifica di leggibilità

- Visualizzazione del documento durante il processo di firma per una verifica sull'operatività dell'utente che sta operando direttamente sul **Signpad/iPad**

- Identificazione automatica dei punti firma
  - Mediante coordinate predefinite
  - Mediante identificazione di un testo predefinito ("ancora") (solo Applet Java)
- Aggiunta di ulteriori punti firma
  - Possibilità da parte dell'Operatore di definire con il mouse ulteriori punti firma ad hoc in base alle esigenze puntuali (solo Applet Java)
- Invio a firma di un documento mediante **Signpad** Signotec o iPad
  - Gestione della visualizzazione del documento sul **Signpad/iPad**
  - Gestione dei pulsanti per l'operatività utente visualizzati sul **Signpad/iPad**
- Processo di acquisizione firme Cliente per i campi firma previsti (dettaglio successivo)
  - Esecuzione della cifratura dei dati
  - Invio dei dati cifrati al Server di gestione
- Verifica automatica della presenza delle firme apposte

E' di seguito riportata la sequenza degli step operativi previsti per l'acquisizione delle firme:

- Il Software Signotec invia al **Signpad** l'hash (Hash1 sha256) del documento
- Durante il rilevamento dei dati biometrici, un secondo hash (Hash 2 sha256) viene generato nel **Signpad** includendo i dati biometrici e le informazioni sul *device*
- Al termine dell'apposizione della firma, i due hash sono combinati e firmati all'interno del **Signpad** con la chiave privata ed inviati al Software Signotec che li include nel file *.pdf*. Informazioni sulla chiave pubblica sono inviate al Software Signotec per consentire di verificare che la firma sia associata al documento corretto.
- I dati biometrici di firma, unitamente ad altri dati tecnici sono criptati all'interno del **Signpad** unitamente all'Hash1, il numero seriale del **Signpad** ed il *time-stamp*. Sono anch'essi inviati al Software Signotec che li include nel file *.pdf*. Tale accorgimento garantisce che i dati biometrici siano associati univocamente al documento originario
- Al termine delle procedure sulle singole firme effettuate, il Software Signotec calcola un terzo hash (Hash 3 sha1) che contiene tutti i dati precedentemente collezionati al fine di essere firmato sul **Signpad** con la chiave privata. Tale step garantisce la compatibilità con lo standard di firma Acrobat Digital Signature. L'hash ricevuto (Hash 3) viene firmato con la chiave privata sul **Signpad** ed inviato al Software Signotec
- Il Software Signotec include nel file *pdf* l'hash documento completo unitamente alla chiave pubblica precedentemente acquisita.

7.5 CHIUSURA DEL DOCUMENTO MEDIANTE FIRMA DIGITALE (C.D. "MASSIVA") DELLA BANCA

Dopo la conferma dell'apposizione dell'ultima firma prevista, il documento viene chiuso mediante firma digitale ("massiva") della Banca i cui certificati sono ospitati in un HSM presso il data-center Banca. I certificati sono della Banca ed emessi sotto la responsabilità di InfoCert che agisce in qualità di Certification Autorithy.

L'apposizione della firma digitale ("massiva") della Banca è tracciata anche visivamente a livello di singolo documento mediante inserimento di apposite diciture che riportino l'informazione sulla presenza di una firma digitale, della data/ora della firma e dell'eventuale Operatore che ha seguito il processo di firma (firma *.pdf* "visibile").

7.6 *INVIO DEL DOCUMENTO AGLI ARCHIVI DOCUMENTALI*

Il documento informatico sottoscritto e chiuso tramite firma della Banca viene inviato tramite canali sicuri a:

- il "Sistema documentale interno di Deutsche Bank S.p.A" gestito da Microdata per consentirne la visualizzazione ai fini operativi da parte della Banca:
  - A seguito di un processo di "flattering" (cancellazione dei dati biometrici), la documentazione inviata presso tale sistema non contiene al suo interno i Dati Biometrici del Cliente ma la firma è visibile solo sottoforma di tratto grafico;
  - La documentazione è accessibile alle strutture operative della banca per consentire l'erogazione del servizio / prodotto e per eventuale attività di assistenza e controllo.

- il "Sistema di gestione documentale per la consultazione della documentazione da parte della Clientela" gestito da Microdata:
  - La documentazione inviata presso tale sistema non contiene al suo interno i Dati Biometrici del Cliente;
  - La consultazione della documentazione da parte della Clientela contiene tramite il servizio db Interactive nell'area MyDocuments ovvero fruibile all'interno dei servizi internet dbDocumentiOnline, nonché db Interactive (internet banking) per i clienti che hanno attivato tale servizio.

- l'archivio di conservazione a norma gestito da InfoCert per la relativa conservazione:
  - La documentazione inviata presso tale sistema contiene al suo interno, in modalità cifrata, i Dati Biometrici del Cliente e non è accessibile alla Clientela ma solamente ad utenti designati della Banca.

8. IL PROCESSO OPERATIVO DI FIRMA ELETTRONICA AVANZATA (OFFERTA FUORI SEDE)

Viene di seguito riportato il processo operativo di firma nella sua interezza.

8.1 *IDENTIFICAZIONE DEL CLIENTE*

1. Il soggetto incaricato dell'offerta fuori sede ("Operatore"), identifica il Cliente mediante (i) riscontro di un documento d'identità o di altro documento di riconoscimento equipollente ai sensi della normativa vigente, (ii) acquisizione della fotografia del documento di identità e del codice fiscale tramite l'utilizzo del tablet (iPad) e (iii) upload delle immagini fotografiche tramite software dedicato. I nominativi ed i dati dell'operatore che opera fuori sede sono compilati ed inclusi automaticamente all'interno dei contratti stessi. Successivamente opera con il Cliente tramite l'utilizzo del tablet (iPad) in cui è disponibile sotto rete protetta aziendale l'app-web di SportelloWEB e l'app di firma grafometrica (fornita da INFOCERT Spa denominata "db La Mia Firma").

8.2 *SOTTOSCRIZIONE DELL'ADESIONE AL SERVIZIO DI FIRMA ELETTRONICA AVANZATA (db La Mia Firma)*

2. Qualora il Cliente acconsenta all'utilizzo della firma grafometrica, sottoscrive su supporto cartaceo il contratto per l'utilizzo del servizio di firma elettronica avanzata ("db La Mia Firma") (per "firma grafometrica" si intende una soluzione di firma elettronica avanzata in forma grafometrica erogata dalla Banca e realizzata da Infocert s.p.a. che comporta il trattamento di dati biometrici comportamentali derivanti dalla sottoscrizione del Cliente) e il

contratto si conclude mediante proposta della Banca e accettazione del Cliente. Lo specimen della sottoscrizione grafometrica del Cliente è raccolto all'interno dell'app-web di "SportelloWEB" su documento di enrolment, dove il Cliente appone 7 sottoscrizioni grafometriche.

8.3 OPERATIVITÀ SUL SISTEMA DI SPORTELLO, TRAMITE WEB-APP SU SUPPORTO TABLET (IPAD DELLA BANCA)

3. L'Operatore, in base ai prodotti o servizi richiesti dal nuovo Cliente, richiede le sottoscrizioni rilevanti all'interno del sistema di sportello, tramite l'utilizzo del suo iPad. In particolare, l'Operatore procede:

    - Alla raccolta dei dati anagrafici del Cliente;

    - A richiedere al Cliente di scegliere l'invio automatizzato via email (all'indirizzo contenuto in anagrafe) della documentazione precontrattuale relativa ai prodotti e ai servizi di cui il Cliente intende usufruire (tale documentazione viene inviata via email al Cliente e conservata dalla Banca nella cartella relativa al Cliente nel repository di Microdata;

    - A richiedere al Cliente di scegliere i rapporti che intende aprire con la Banca (il servizio di Home Banking db Interactive ed il servizio di firma grafometrica risulteranno preselezionati, poiché anche se facoltativi per il Cliente, essi risultano obbligatori nel processo tramite iPad); il Cliente ovviamente in qualsiasi momento può interrompere il processo di apertura di un rapporto

4. Al termine dell'apertura dei rapporti selezionati, e prima della firma dei contratti, vengono inviati automaticamente i seguenti documenti alla casella email comunicata dal Cliente:

    - Fascicolo contrattuale, che a breve il Cliente va a sottoscrivere, dei prodotti richiesti (contiene tutti i dati anagrafici e di prodotto censiti nella fase appena conclusa), inclusi tutti i Documenti di Sintesi relativi agli stessi prodotti
    - Contratto Quadro del Conto Corrente, dei Servizi Aggiuntivi, delle Operazioni di Pagamento, del deposito di strumenti finanziari e per la prestazione di servizi di investimento
    - Kit Mifid (se incluso il Dossier Titoli)
    - Guida al db Interactive
    - Guida pratica al c/c (ABI)
    - Guida pratica per l'accesso all'Arbitro Bancario Finanziario

5. La Banca acquisisce l'attestazione del Cliente circa l'avvenuta consegna dei documenti sopra indicati ai sensi della normativa vigente, mediante sottoscrizione con firma grafometrica dell'apposita dichiarazione da parte dello stesso.

8.4 OPERATIVITÀ DI FIRMA GRAFOMETRICA SULL'APP PER IPAD "db La Mia Firma"

6. Dopo che sono stati raccolti i dati anagrafici del Cliente e dopo che lo stesso Cliente ha indicato i prodotti o i servizi di cui intende usufruire, l'Operatore, dal suo iPad, apre l'app di firma grafometrica "db La Mia Firma". L'app consente il riconoscimento automatico

dell'Operatore in base alle credenziali interne fornite dallo stesso in fase di login alla rete protetta (VPN).

7. L'app è installata all'interno dei data center della Banca e fruibile solo all'interno della rete intranet di DB per i soggetti aventi profili abilitati.

8. La documentazione che deve essere sottoscritta dal Cliente tramite firma grafometrica è disponibile all'interno dell'applicativo di sportello della Banca che ne garantisce l'integrità, la completezza e la sicurezza in base alle policy della Banca.

9. L'Operatore accede all'applicazione di firma grafometrica per l'operatività richiesta e procede alle seguenti attività:
    - Visualizzazione della pratica
    - Verifica della documentazione richiesta
    - Visualizzazione dei documenti acquisiti automaticamente
    - Aggiunta di documenti del Cliente mediante fotocamera dell'iPad
    - Avvio dell'operatività di firma grafometrica.

10. L'applicativo di sportello è connesso all'iPad dell'Operatore, mediante collegamento intranet in modalità cifrata: l'eventuale assenza di una connettività interna (network) comporta il blocco sia della rilevazione dei dati biometrici da parte dell'app di firma che di tutte le funzionalità dell'applicativo di firma grafometrica.

11. Il documento elettronico in formato .pdf è inviato allo schermo dell'iPad attraverso l'app di firma grafometrica su richiesta dell'Operatore affinché lo stesso documento sia pronto per essere firmato dal Cliente. L'Operatore, durante il processo di firma grafometrica, ha la possibilità di visualizzare il documento presente sull'iPad in modo da verificare l'apposizione della sottoscrizione grafometrica da parte del Cliente.

12. Il Cliente prende visione del documento elettronico che intende sottoscrivere e ha la possibilità di scorrere attraverso le pagine dello stesso, ingrandire o rimpicciolire il carattere per la lettura. Dopo aver terminato la lettura ed eventualmente dopo aver richiesto opportuni chiarimenti e spiegazioni all'Operatore, il Cliente conferma la propria volontà di sottoscrivere i documenti posti dinanzi a lui selezionando e apponendo su ciascun punto firma la propria firma grafometrica (eventualmente anche tramite pennino su iPad) che permette di raccogliere i dati biometrici comportamentali del Cliente: (congiuntamente, "Dati Grafometrici", contestualmente all'apposizione della firma).

13. Il perimetro dei prodotti e servizi che possono essere offerti al Cliente e la cui documentazione contrattuale può essere sottoscritta dal Cliente tramite firma grafometrica, può variare in relazione alla qualifica dell'Operatore: (i) l'Operatore senza la qualifica di consulente finanziario abilitato all'offerta fuori sede può proporre al Cliente l'apertura dei seguenti prodotti o servizi: firma grafometrica, conto corrente, home banking ("db Interactive") e carta bancomat; (ii) l'Operatore con la qualifica di consulente finanziario abilitato all'offerta fuori sede, in aggiunta ai già menzionati prodotti e servizi, può promuovere altresì servizi di investimento e altri servizi accessori.

14. Dopo il perfezionamento dei contratti relativi ai servizi bancari o di investimento che il Cliente ha inteso aprire, il Cliente può impartire ordini esecutivi (ad esempio ordini di pagamento e/o ordini di acquisto di strumenti finanziari), mediante sottoscrizione dei relativi moduli con firma grafometrica.

15. Il Cliente ha il controllo esclusivo del processo di firma grafometrica e dispone delle seguenti funzioni:
    - visualizzazione integrale del documento;
    - avvio del processo di firma;
    - conferma della firma apposta;
    - riapposizione della firma in caso di errore;
    - annullamento dell'inserimento di una singola firma o di tutte le firme apposte su un documento;
    - annullamento di ogni operazione e revoca del consenso al trattamento dei dati anagrafici o biometrici.

16. Mentre il Cliente appone la firma, i Dati Grafometrici vengono immediatamente cifrati e inclusi nei documenti sottoscritti. Tali documenti vengono progressivamente messi a disposizione del Responsabile di Sportello (o suo facente funzione) della filiale di riferimento per gli adempimenti successivi.

17. I Dati Grafometrici sono cifrati all'interno dell'iPad avvalendosi di un software dedicato e caricati automaticamente nell'Applet Signotec. L'Applet Signotec recepisce i dati cifrati e li inserisce all'interno del documento selezionato dal Cliente per la sottoscrizione in formato .pdf. (vedasi paragrafo "Tecnologia abilitante Signotec" nel presente documento)

18. Al termine della apposizione della firma grafometrica da parte del Cliente, sono generate una serie di stringhe hash per la successiva verifica dell'integrità della firma in caso di contestazione da parte del Cliente nell'ambito di un contenzioso avanti l'autorità giudiziaria e dei documenti acquisiti in formato elettronico, anch'esse cifrate con la chiave pubblica installata nel dispositivo, con algoritmo RSA. A questo punto:
    - (i) il Cliente ha ricevuto via email la documentazione pre-contrattuale;
    - (ii) il Cliente procede alla sottoscrizione del contratto ed ottiene evidenza dei documenti firmati grafometricamente già al momento della apposizione della firma grafometrica, nella sezione dei contratti firmati all'interno dell'app di firma grafometrica, disponibile sull'iPad dell'Operatore. Lo stesso Cliente riceve via email la documentazione sottoscritta.
    - (iii) il Cliente da atto mediante attestazione sottoscritta con firma grafometrica di aver ricevuto copia della suddetta documentazione via email.

19. Se i sottoscrittori sono più di uno o sono richieste più firme del medesimo soggetto, l'Operatore richiede ai clienti sottoscrittori o al Cliente sottoscrittore di ripetere le operazioni sopra descritte per ciascuna firma necessaria, eventualmente anche in tempistiche differenti.
    In caso di cointestazione dei rapporti, ognuno dei co-intestatari deve apporre la propria firma grafometrica in ognuno dei punti firma della documentazione rilevante. La documentazione si può dire correttamente firmata solo con l'apposizione di tutte le sottoscrizioni richieste per tutti i cointestatari. Poiché il servizio "db La Mia Firma" è facoltativo, qualora taluno dei cointestatari non intenda aderire al servizio "db La Mia Firma", nessuno dei cointestatari può avvalersi del servizio "db La Mia Firma".

20. Prima di ogni successiva operazione di firma, SportelloWEB verifica automaticamente se il Cliente ha sottoscritto su supporto cartaceo il contratto relativo al servizio "db La Mia Firma". In caso di verifica positiva il Cliente può sottoscrivere altri documenti. In caso di verifica

negativa è necessario sottoporre al Cliente su supporto cartaceo il contratto per l'utilizzo del servizio "db La Mia Firma".

8.5 *LA FIRMA DELLA BANCA*

21. Dopo aver raccolto il consenso del Cliente all'utilizzo della firma grafometrica, effettuato l'upload delle "fotografie" dei documenti per l'identificazione, nonché dei contratti e dei moduli sottoscritti dal Cliente mediante firma grafometrica, l'Operatore, tramite pulsante dedicato sull'app di firma, mette a disposizione sulla dashboard del Responsabile di Sportello (o suo facente funzione) la pratica.

22. Il Responsabile di Sportello (o suo facente funzione), dalla sua postazione in Filiale e tramite tramite l'applicativo di sportello, riceve un avviso della presenza di una proposta contrattuale di un Cliente da valutare.

23. Lo stesso Responsabile accede quindi, tramite la sua postazione e sul suo computer, alla sua dashboard di firma su cui visualizza la specifica proposta contrattuale e tutta la documentazione necessaria per lo svolgimento dei suoi controlli sostanziali e sull'operato dell'Operatore.

24. In particolare, il Responsabile dello Sportello (o suo facente funzione):
    - prende in carico e analizza la pratica unitamente ai documenti allegati;
    - verifica la correttezza della documentazione;
    - (se munito dei poteri) avvia il procedimento di firma digitale ("massiva") in nome e per conto della Banca per l'accettazione dei contratti.

8.6 *INVIO DELLA PROPOSTA CONTRATTUALE AI SISTEMI DOCUMENTALI*

25. La proposta contrattuale sottoscritta dal Cliente e dalla Banca insieme alla documentazione accessoria necessaria all'apertura del rapporto viene inviata tramite canali sicuri:

    - al "Sistema documentale interno di Deutsche Bank S.p.A" gestito da Microdata (tali copie informatiche dei documenti sottoscritti dal Cliente risultano prive dei dati biometrici dei clienti in quanto il loro utilizzo ha il solo scopo di visualizzazione ai fini operativi da parte della Banca);
    - al Sistema documentale per la consultazione della documentazione da parte della Clientela tramite Home Banking (tramite il servizio db Interactive nell'area MyDocuments), gestito da Microdata; (copie informatiche dei documenti sottoscritti dal Cliente)
    - all'archivio di conservazione a norma gestito da InfoCert (documenti provvisti di dati biometrici, che costituiscono duplicati informatici dei documenti sottoscritti dai clienti);

8.7 *ACCETTAZIONE DELLA BANCA*

26. La Banca accetta la proposta del Cliente secondo le seguenti modalità:

    - il Responsabile di Sportello (o suo facente funzione), avvia il processo di firma digitale ("massiva") da parte del Country Operative Officer (ossia il legale rappresentante della Banca) per procedere alla sottoscrizione in nome e per conto

della Banca su ciascun punto firma di ogni proposta contrattuale firmata grafometricamente dal Cliente;

- Il documento così controfirmato viene inviato al Cliente sul canale home banking (il Cliente riceve anche una email che lo informa della ricezione su MyDocuments dell'accettazione della Banca);

- Per ottenere una conferma della conoscenza dell'accettazione da parte del Cliente direttamente su db Interactive la Banca conserva la tracciabilità della visualizzazione da parte del Cliente (mediante appositi file di log conservati dalla Banca) del documento contenente l'accettazione della Banca;

- Il certificato di firma e relativa chiave privata sono ospitati su un HSM sotto la responsabilità di InfoCert che agisce in qualità di Certification Autorithy;

- l'HSM è installato presso il data center Banca;

- Tale gestione è identica a quella già in funzione e disponibile per le pratiche di firma grafometrica concluse in filiale.

9. LA GESTIONE E PROTEZIONE DELLA MASTER KEY

Le chiavi di cifratura sono basate su certificati digitali emesse da InfoCert che agisce in qualità di C.A.
Dopo la creazione della coppia di chiavi RSA e del relativo certificato, secondo lo standard X.509, in un ambiente protetto, alla presenza di un notaio, del funzionario della sicurezza di DB e dell'amministratore dei sistemi di C.A., la chiave privata è caricata su 5 (cinque) dispositivi sicuri e, in formato PKCS#12, sul sistema di conservazione a norma InfoCert. Il notaio imposta la *password* di protezione per la cifratura delle chiavi, del PKCS#12 e delle credenziali dei dispositivi sicuri.
I dispositivi contenenti la chiave sono inseriti in buste sigillate conservate dal notaio stesso; per ogni busta corrispondono altrettante buste sigillate (in duplice copia) per il PIN/PUK dei dispositivi e per la *password* del PKCS #12.

Le buste sigillate sano così distribuite:

- Le buste contenenti 3 (tre) dispositivi sicuri sono conservate all'interno della cassaforte del bunker C.A. (un dispositivo per la successiva eventuale operazione di verifica egli altri due come copie di sicurezza).
- Due copie di sicurezza dei dispositivi sono inviati nel sito di DR e conservati nella relativa cassaforte.
- Tutte le buste contenti i PIN/PUK e le Passphrase di protezione sono consegnate al Notaio che le custodisce opportunamente presso di sé.

Il Notaio redige e firma, assieme ai soggetti presenti, il verbale delle operazioni, che è conservato nel sistema di conservazione a norma InfoCert.

10. STRUMENTI E PROCEDURE PER L'ANALISI GRAFOLOGICA

Il processo di decifratura, che consente di risalire ai Dati Grafometrici in chiaro dell'utente, può essere eseguito solo se si è in possesso della chiave privata di cifratura custodita da InfoCert, che la rende disponibile solo su richiesta del legale rappresentante della Banca conseguente ad un ordine dell'autorità giudiziaria, nell'ambito di un contenzioso promosso dal Cliente.

10.1 PROCEDURE PER L'ANALISI GRAFOLOGICA

Le procedure di dettaglio sono di seguito sinteticamente riportate.

Ipotesi preliminari:

- Viene predisposta una nuova postazione dedicata in base alle caratteristiche tecnologiche e di sicurezza previste all'interno della quale sono approntati i Software minimali e le utenze per l'esecuzione delle attività.
- Il documento da peritare è estratto dal sistema di conservazione a cura dell'Azienda/Ente, e portato fisicamente sulla macchina tramite un qualsiasi supporto di memoria rimovibile (chiave USB standard).
- Il funzionario della sicurezza della *Certification Authority*, dopo aver verificato la presenza di tutti stakeholder necessari con i relativi supporti (CD), si accorda con il Notaio per l'esecuzione delle procedura.

Accedendo alla postazione attraverso l'utenza dedicata si procede:

- Alla verifica e all'apertura della busta contente il dispositivo sicuro conservati da InfoCert, se il Software di verifica presente nella WS è in grado di accedervi col protocollo PKCS#11 ovvero all'esibizione dal sistema di conservazione a norma del certificato PKCS#12
- Alla verifica e all'apertura della busta delle password /PIN portata con sé dal Notaio
- All'avvio dello strumento Software di verifica;
- Al caricamento del documento da verificare da supporto esterno;
- Allo sblocco della chiave di decifratura con le credenziali da parte del Notaio;
- All'effettuazione della Perizia da parte del Perito grafologo nominato dall'azienda/ente;
- Al cambio password della Master Key, eseguito dal Notaio. Alla presenza al responsabile dell'azienda/ente e del Notaio si provvede al cambiamento della password di protezione utilizzata in precedenza.

E' a cura del Perito la redazione del documento di perizia, anche presso il proprio studio con i dati raccolti. Nel caso il Perito non abbia terminato la perizia o non sia presente, il Notaio ha a disposizione un Software di cifratura con cui, impostata a sua scelta una password, cifra i documenti decifrati precedentemente, e li rende disponibili al soggetto indicato dal Cliente assieme alla chiave di decifrazione.

Al termine il funzionario della sicurezza della C.A. richiede al Notaio di impostare nuovi PIN/PUK per il dispositivo sicuro utilizzato o una nuova PSW per il PKCS#12, distrugge le buste utilizzate e consegna le nuove buste prodotte. Il Notaio verifica l'integrità delle nuove buste le conserva presso i propri Uffici.

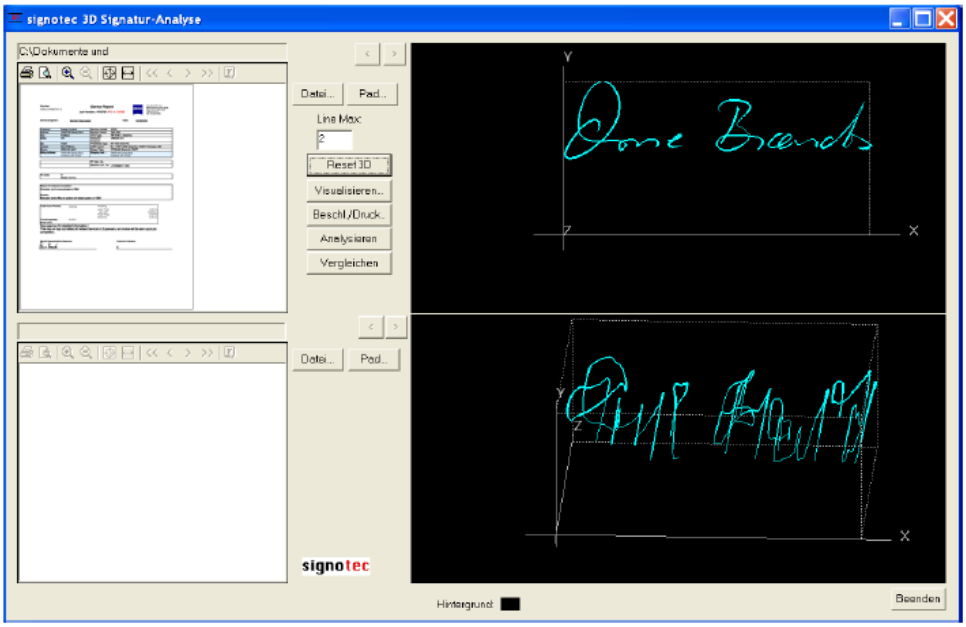
Il funzionario C.A. effettua il resoconto delle operazioni, che è sottoscritto da tutti i partecipanti.

10.2 STRUMENTI PER L'ANALISI GRAFOLOGICA

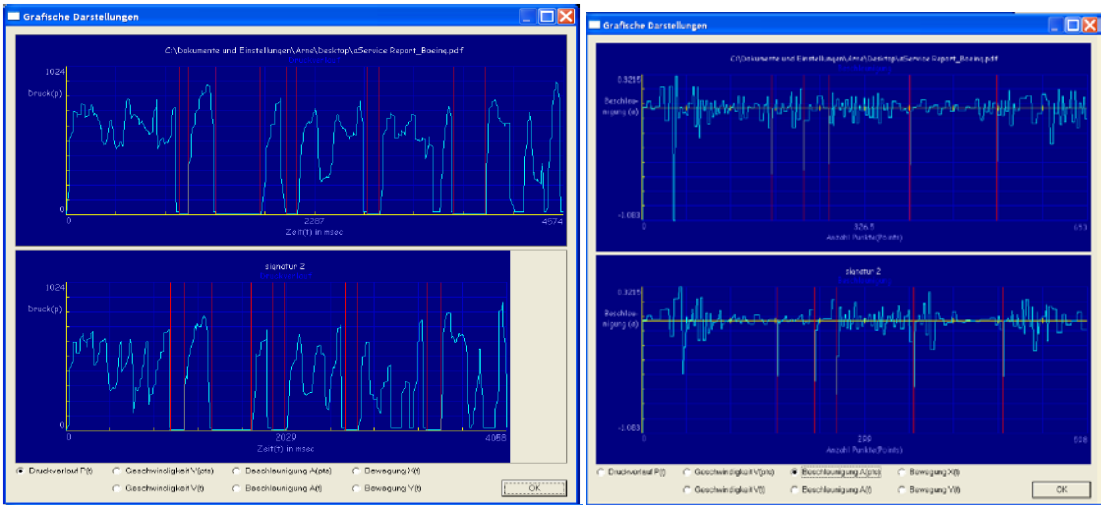
Signotec mette a disposizione uno specifico programma per l'analisi dei dati grafometrici a supporto dei periti calligrafi per consentire le operazioni di verifica di autenticità di una firma.

Si riportano di seguito alcune schermate del programma:

Deutsche Bank



Visualizzazione della firma e dei vettori di firma



Visualizzazione andamento singole dimensioni biometriche