Firma Elettronica Avanzata in modalità Grafometrica

Documento riassuntivo delle caratteristiche tecniche del Servizio

Allianz Bank
Financial Advisors

1 Introduzione al documento

1.1 Scopo e campo di applicazione

Il presente documento contiene tutte le informazioni obbligatorie, di tipo tecnico e organizzativo, per consentire la piena aderenza alle regole tecniche di firma elettronica avanzata.
Il documento è referenziato dal **Modulo di Attivazione del Servizio di "FirmaSmart Tablet"** (di seguito anche **Modulo di Attivazione**) e rappresenta il documento riassuntivo delle caratteristiche tecniche del servizio di firma elettronica.

1.2 Riferimenti normativi e tecnici

Riferimenti normativi

1) Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (GU n. 42 del 20 febbraio 2001) – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
2) Decreto Legislativo 7 marzo 2005, n. 82 (GU n. 112 del 16 maggio 2005) – Codice dell'Amministrazione Digitale e successive modifiche e integrazioni, di seguito referenziato come **CAD**
3) Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 (GU n.117 del 21 maggio 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, di seguito referenziato come **DPCM**
4) Deliberazione CNIPA numero 45/2009 (GU n. 282 del 3 dicembre 2009) – Regole per il riconoscimento e la verifica del documento informatico
5) Determinazione Commissariale DigitPA N. 69/2010 (GU n. 191 del 17 agosto 2010) – Modifiche alla Deliberazione 21 maggio 2009 n. 45 del Centro Nazionale per l'Informatica nella pubblica Amministrazione, recante "Regole per il riconoscimento e la verifica del documento informatico"
6) Decreto Legislativo 30 giugno 2003, n. 196 (GU n. 174 del 29 luglio 2003) – Codice per la protezione dei dati personali
7) Decreto Legislativo n.231 del 21 novembre 2007 (GU n.290 del 14 dicembre 2007) – "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione"
8) Ufficio Italiano Cambi: parere del 14 giugno 2001
9) Provvedimento di Banca d'Italia dell'11 aprile 2013 – Provvedimento recante disposizioni attuative in materia di adeguata verifica della clientela, ai sensi dell'art. 7, comma 2, del Decreto Legislativo 21 novembre 2007, n. 231
10) Deliberazione CNIPA n. 11 del 19 febbraio 2004 (GU n. 57 del 9 marzo 2004) – Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - Art. 6, commi 1 e 2, del testo

unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

11) Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 (GU n.59 del 12-3-2014) - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al Decreto Legislativo n. 82 del 2005.

1.3 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal **CAD** e dal **DPCM** si rimanda alle definizioni in essi stabilite. Dove appropriato, viene indicato tra parentesi quadre il termine inglese corrispondente, generalmente usato nella pubblicistica, negli standard e nei documenti tecnici.

Certificato Qualificato	• Il certificato elettronico conforme ai requisiti di cui all'allegato I della Direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva (art 1, comma 1 lettera f **CAD**).
Certificato, Certificato Digitale	• Insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica. • Nel certificato compaiono altre informazioni tra cui: o il Certificatore che lo ha emesso o il periodo di tempo in cui il certificato può essere utilizzato; o altri campi (estensioni) che determinano caratteristiche aggiuntive al certificato.
Certificatore [Certification Authority]	• Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime (art 1, comma 1 lettera g **CAD**.)
Chiave privata	• L'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico. Art comma lettera h **CAD**. • Nei processi di cifratura di dati è l'elemento segreto che serve a decifrare i dati cifrati.
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 (art 1, comma 1 lettera i **CAD**). • Nei processi di cifratura di dati è l'elemento inserito nel sistema che è utilizzato per i dati raccolti, ad esempio i dati biometrici connessi alla firma grafometrica.
Conservazione / Conservazione a norma	• Processo di archiviazione sicura a lungo termine di documenti informatici o copie per immagine di documenti analogici, che ne assicura l'integrità, la sicurezza, l'immodificabilità, la disponibilità e il mantenimento del valore legale.
Copia informatica di documento informatico	• Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari (art 1, comma 1 lettera i-quater **CAD**).

Copia per immagine di documento analogico	• Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto (art 1, comma 1 lettera i-ter **CAD**).
Duplicato informatico	• Il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario (art 1, comma 1 lettera i-quinquies **CAD**).
Evidenza informatica	• Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (articolo 1, co. 1, lettera f **DPCM**).
Firma digitale	• Un particolare tipo di firma elettronica avanzata 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 (art 1, comma 1 lettera s **CAD**.)
Firma elettronica	• L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (art 1, comma 1 lettera q **CAD**.)
Firma elettronica avanzata	• Insieme di dati in forma elettronica allegati oppure connessi a un documenti 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 il 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 (art 1, comma 1 lettera q-bis **CAD**)
Firma elettronica qualificata	• Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art 1, comma 1 lettera r **CAD**)
Firma Grafometrica	• Un particolare tipo di firma elettronica ottenuta grazie al rilevamento dinamico dei dati calligrafici (ritmo, pressione, velocità, inclinazione della penna, movimento, ecc.) della firma di un individuo tramite una penna elettronica su specifici dispositivi idonei a rilevare le caratteristiche sopra indicate.
Hash / impronta	• La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione a una evidenza informatica di una opportuna funzione di hash (articolo 1, co. 1, lettera h **DPCM**)
Funzione di hash	• Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguale a partire da evidenze informatiche differenti (articolo 1, co. 1, lettera g **DPCM**)
Marca temporale (Time Stamp Token)	• Il riferimento temporale che consente la validazione temporale (articolo 1, co. 1, lettera i **DPCM**)
Modulo di Attivazione del Servizio di "FirmaSmart Tablet"/ Modulo di Attivazione	• Documento contrattuale elaborato da Allianz Bank Financial Advisors SpA che raccoglie i consensi del cliente in merito alla privacy e all'utilizzo del sistema di firma elettronica, in relazione ad ogni contratto stipulato dal Cliente con la Banca.
Pad di firma	• Dispositivi per postazione fissa, collegati a mezzo cavo USB a un PC, con cui si raccolgono i dati biometrici.
PDF/A	• Standard internazionale (ISO 19005-1), sottoinsieme dello standard PDF, appositamente pensato per l'archiviazione nel lungo periodo di documenti elettronici in quanto garantisce che il documento sia visualizzabile sempre allo stesso modo, anche a distanza di tempo e con programmi software diversi

Rendering	• Copia informatica di documento informatico con contenuto e forma uguali a quello del documento di partenza, che non contiene gli elementi biometrici, di firma digitale o di marca temporale.
Responsabile della Conservazione	• Soggetto responsabile del sistema di conservazione dei documenti
Tablet	• Tablet pc dotati di connettività che consentono di visualizzare direttamente il documento e raccogliere la firma del cliente e i parametri biometrici connessi.
XML	• Extensible Markup Language, metalinguaggio utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati.

2 Generalità

La fattispecie "firma elettronica avanzata" è stata introdotta nel nostro ordinamento dal decreto legislativo 30 dicembre 2010, n. 235 di modifica del codice dell'amministrazione digitale (il d.l.vo n. 82/2005, **CAD**), che ha inserito una nuova definizione alla lettera q-bis) dell'art. 1: "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".
Dal punto di vista probatorio, il medesimo decreto legislativo n. 235/2010 ha inoltre stabilito che:
"Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile[1]."

Per poter sostanziare nella pratica una Firma Elettronica Avanzata (di seguito anche "**FEA**"), è necessario il rispetto delle regole tecniche di cui al DPCM 22 febbraio 2013 pubblicato nella Gazzetta Ufficiale n. 117 del 21 maggio 2013.

In questo contesto si inserisce la fattispecie di firma grafometrica, ossia un particolare tipo di firma elettronica che si ottiene dal rilevamento dinamico dei dati calligrafici (ritmo, pressione, velocità, inclinazione della penna, movimento, ecc.) della firma di un individuo tramite una penna elettronica.
La firma grafometrica viene apposta tramite l'utilizzo di specifici "tablet", idonei a rilevare le caratteristiche sopra indicate dei dati calligrafici che costituiscono i "dati biometrici" del sottoscrittore. La soluzione di firma grafometrica, a fronte di un valido riconoscimento del sottoscrittore, deve consentire di assicurare il rispetto dei requisiti per la validità della firma elettronica avanzata.

Questo documento evidenzia le regole generali e le procedure seguite dal Soggetto Erogatore Allianz Bank Financial Advisors SpA (nel prosieguo semplicemente indicato come Allianz Bank) per l'erogazione e l'utilizzo del servizio di Firma Elettronica Avanzata in modalità grafometrica.

2.1 Attori

2.1.1 Soggetto Erogatore

Allianz Bank è il Soggetto Erogatore della soluzione di FEA come definito dall'articolo 55 comma 2 lettera a del **DPCM**.

[1] Art. 2702 Efficacia della scrittura privata: La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa e legalmente considerata come riconosciuta.

2.1.2 Financial Advisors Allianz Bank

Nello svolgimento delle proprie attività di Soggetto Erogatore, Allianz Bank si avvale sul territorio di Financial Advisors che svolgono principalmente le funzioni di:

- Identificazione del Firmatario;
- Raccolta della copia del documento di identità;
- Sottoscrizione della dichiarazione di adesione al servizio di Firma Grafometrica (Modulo di Attivazione);
- Supporto al Firmatario nell'apposizione della firma, nella fornitura e revoca del consenso.

I Financial Advisors sono attivati dal Soggetto Erogatore a seguito di un adeguato addestramento.
Per il dettaglio dei Financial Advisors si rimanda al tool di ricerca disponibile sul sito di Allianz Bank[2].

2.1.3 Soggetto Realizzatore

InfoCert è il Soggetto Realizzatore della soluzione di FEA come definito dall'articolo 55 comma 2 lettera b) del **DPCM**, che eroga i servizi di firma grafometrica grazie alla piattaforma installata presso il proprio data-center.
InfoCert è il Primo Ente Certificatore per la firma digitale in Italia, leader di mercato per i processi di conservazione sostitutiva dei documenti a norma di legge e per i servizi di Posta Elettronica Certificata. InfoCert progetta e sviluppa soluzioni informatiche ad alto valore tecnologico per la dematerializzazione dei processi documentali di imprese, associazioni, ordini professionali, Pubblica Amministrazione e professionisti.
Con un capitale sociale di 17.704.890 euro, InfoCert eroga servizi di gestione documentale, conservazione sostitutiva a norma dei documenti, certificazione e sicurezza digitale, gestione di Posta Elettronica Certificata, dematerializzazione dei flussi documentali end-to-end, firma elettronica avanzata, qualificata e digitale.

InfoCert è in possesso della certificazione di conformità del proprio sistema di gestione per la sicurezza delle informazioni ad essi relative alla norma ISO/IEC 27001, e della certificazione di conformità del proprio sistema di qualità alla norma ISO 9001, ponendosi in linea con quanto previsto, per le pubbliche amministrazioni, dall'articolo 58 commi 1 e 2 del **DPCM**.

Nella soluzione di FEA, InfoCert svolge anche il ruolo di Certification Authority di riferimento per l'acquisizione degli strumenti certificati di firma digitale e cifratura che intervengono nel processo.
InfoCert svolge il ruolo di Responsabile della Conservazione dei documenti in base all'atto di affidamento a questo scopo sottoscritto da Allianz, per la delega dei compiti e delle responsabilità ad InfoCert come soggetto terzo dotato di adeguata competenza ed esperienza, ai sensi della deliberazione CNIPA 11/04, articolo 5, comma 2.

InfoCert è inoltre la terza parte fidata cui è affidata la custodia della chiave di decifratura dei dati biometrici, elemento essenziale nei processi di verifica della firma.

Denominazione Sociale	**InfoCert SpA**

[2] http://www.allianzbank.it/contatta-promotore

Sede Legale	Piazza Sallustio, 9 – 00187 Roma
Sedi Operative	Via Marco e Marcelliano, 45 – 00147 Roma Via Russoli, 5 – 20143 Milano Corso Stati Uniti, 14 – 35127 Padova
Partita IVA	07945211006
Numero iscrizione Registro delle Imprese	RM – 1064345
Sito Web	www.infocert.it
PEC	infocert@legalmail.it

3 Regole Generali

3.1 Obblighi e Responsabilità

In questo capitolo si descrivono le condizioni generali con cui Soggetto Erogatore Allianz Bank eroga il servizio di Firma Elettronica Avanzata descritto in questo documento.

3.1.1 Obblighi del Sottoscrittore

Il Firmatario è tenuto a garantire:

a) La correttezza e la completezza dei dati personali forniti;
b) La consegna al Financial Advisor o all'incaricato di Allianz Bank di un documento di identità in corso di validità al momento della sottoscrizione del Modulo di Attivazione;
c) Di aver preso visione della documentazione descrittiva del servizio FEA prima dell'adesione al servizio;
d) L'utilizzo del servizio FEA sviluppato da Allianz Bank solamente nell'ambito dei rapporti giuridici intercorrenti tra Allianz Bank e il Firmatario stesso.

3.2 Assicurazione obbligatoria

Ai sensi dell'articolo 57 comma 2 Allianz Bank ha stipulato una idonea copertura assicurativa per la responsabilità civile, nel rispetto dei massimali previsti dal DPCM.

4 Identificazione del Sottoscrittore

Ai sensi dell'articolo 57 comma 1 lettera a) del **DPCM**, i soggetti erogatori della soluzione di FEA devono identificare in modo certo l'utente tramite un valido documento di riconoscimento al fine di configurare una firma elettronica avanzata correttamente formata.
In questo capitolo si descrivono le modalità di identificazione, i soggetti abilitati e il processo di identificazione facente parte della soluzione di FEA Grafometrica Allianz Bank.

4.1 Identificazione ai fini dell'adesione

L'identificazione certa del firmatario del documento è eseguita per Allianz Bank dai soggetti indicati al successivo §4.2 ed è richiesta la presenza fisica del Firmatario. Nei casi previsti dalla legge, la procedura di identificazione ai fini FEA coincide con quella di identificazione ai sensi antiriciclaggio, eseguita ai sensi del D.Lgs 231/2007 (7)) sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente.

4.2 Soggetti abilitati ad effettuare l'identificazione

I soggetti abilitati ad effettuare l'identificazione sono i Financial Advisors Allianz Bank presenti sul territorio[3], secondo la procedura di identificazione definita e validata dalla stessa Allianz Bank.

[3] Si rimanda al sito di Allianz Bank (http://www.allianzbank.it/contatta-promotore) per il dettaglio geografico della rete di Financial Advisor.

5 Operatività

5.1 Identificazione e adesione alla modalità di firma

Il processo di identificazione del sottoscrittore e adesione alla modalità di firma è eseguito una tantum al primo utilizzo del servizio di firma elettronica e si compone delle seguenti fasi:

1. Il Financial Advisor controlla a sistema che per il cliente siano già state svolte tutte le attività previste ai sensi della normativa antiriciclaggio e dei relativi regolamenti attuativi vigenti ("Adeguata verifica") e che, conseguentemente, sia stata raccolta copia del documento di identità, valido alla data di attivazione del servizio (già archiviata in formato cartaceo presso Allianz Bank).;
2. Le applicazioni di Allianz Bank generano il Modulo di Attivazione in PDF, che viene sottoposto alla firma del sottoscrittore tramite tablet;
3. Il cliente è invitato a leggere su tablet il Modulo di Attivazione e a sottoscriverlo con la firma grafometrica;
4. La piattaforma di firma grafometrica raccoglie i dati biometrici e li inserisce cifrati all'interno del Modulo di Attivazione in PDF;
5. La piattaforma di firma grafometrica appone una firma digitale automatica, appartenente a procuratori autorizzati di Allianz Bank, e una marca temporale al Modulo di Attivazione sottoscritto**,**;
6. Il sistema invia all'indirizzo elettronico dichiarato dal Cliente nel Modulo di Attivazione un file in formato PDF contenente l'immagine del documento sottoscritto e della sottoscrizione apposta (rendering).;
7. La piattaforma di firma grafometrica invia il Modulo di Attivazione sottoscritto al sistema di Conservazione Elettronica a Norma InfoCert per i 20 anni previsti dall'articolo 57 comma 1 lettera b) del **DPCM**.

Tutte le variazioni ai dati e alle informazioni, nonché ai consensi forniti, devono essere effettuate compilando nuovamente e sottoscrivendo il Modulo di Attivazione.

Per i contratti e i documenti sottoscritti dopo l'adesione al servizio il Financial Advisor si limiterà ad accertarsi della correttezza dell'identità del Cliente, senza acquisire nuovamente la copia del documento di identità, se in corso di validità.

5.2 Firma del documento

Dopo l'adesione al servizio di firma elettronica avanzata, il processo di sottoscrizione di un documento consta delle seguenti fasi:

1. Il Financial Advisor accede al sistema Allianz Bank attraverso la app installata sul tablet ed elabora la proposta commerciale, che è salvata sugli applicativi Allianz Bank;
2. Il Financial Advisor seleziona la funzione che permette di firmare in modalità grafometrica il documento;
3. Gli applicativi Allianz Bank generano il documento in formato PDF e lo inviano alla piattaforma di firma grafometrica. Il documento è visualizzato sul tablet;

4. Il Cliente prende visione del contratto in tutte le sue parti sfogliandolo mediante le apposite funzionalità (sfoglia il PDF utilizzando le dita sul tablet);
5. Il Cliente appone la propria firma sul documento visualizzato sul tablet utilizzando l'apposito pennino elettronico e conferma;
6. Il pad o il tablet registrano i parametri biometrici associati alla firma ovvero:
   - Velocità orizzontale di scorrimento della penna (asse x)
   - Velocità verticale di scorrimento della penna (asse y)
   - Posizione del pennino sull'asse orizzontale (asse x)
   - Posizione del pennino sull'asse verticale (asse y)
   - Pressione esercitata[4]
   - Accelerazione del pennino
7. I dati biometrici raccolti sono crittografati dalla piattaforma di firma grafometrica utilizzando una chiave pubblica, indi inseriti nel documento PDF insieme a una serie di codici (codici di hash) che consentono di garantire l'immodificabilità del documento nel tempo e l'impossibilità di estrarre i dati biometrici stessi dal PDF per riutilizzarli su un altro documento
8. La piattaforma di firma grafometrica procede all'apposizione di una o più firme digitali appartenenti a soggetti Allianz Bank[5] sul documento con procedura automatica;
9. La piattaforma di firma grafometrica procede all'apposizione di una marca temporale emessa dalla TSA InfoCert sul documento;
10. La piattaforma di firma grafometrica restituisce alle applicazioni Allianz Bank un file in formato PDF contenente l'immagine del documento sottoscritto e della sottoscrizione apposta (*rendering*), che è archiviato. Le applicazioni Allianz Bank inviano il PDF rendering all'indirizzo elettronico dichiarato dal Cliente nel Modulo di Attivazione;
11. La piattaforma di firma grafometrica invia il documento al sistema di conservazione elettronica a norma InfoCert.

5.3 Soluzione tecnologica utilizzata

La soluzione tecnologica utilizzata si compone di tre macro-elementi: la postazione del Financial Advisor con il tablet di raccolta di firma, le applicazioni Allianz Bank di creazione del documento e la piattaforma di firma grafometrica InfoCert, integrata con i servizi di certificazione digitale e conservazione del documento informatico.

5.3.1 Postazione del Financial Advisor

La postazione del Financial Advisor coincide con il il tablet utilizzato per l'operatività, allestito per poter raccogliere la firma grafometrica.
La soluzione tecnologica prescelta utilizza dispositivi hardware dotati di tecnologia *touch* in grado di rilevare i principali parametri della firma dell'utente (si veda § 5.2 punto 6). I dispositivi utilizzati afferiscono alla categoria dei dispositivi mobili:

- Dispositivi mobili: tablet dotati di connettività che consentono di visualizzare direttamente il documento e raccogliere la firma del cliente e i parametri biometrici connessi[6].

[4] In caso di utilizzo del dispositivo Apple Ipad ® non è raccolto il parametro di pressione.
[5] Dipende dal tipo di documento e se lo Statuto Allianz Bank richiede che siano presenti una o due firme
[6] In caso di utilizzo del dispositivo Apple Ipad ® non è raccolto l'indice di pressione.

5.3.2 Applicazioni Allianz Bank

Le applicazioni Allianz Bank, erogate dal data-center della Compagnia, consentono la gestione della trattativa commerciale, l'inserimento della proposta, dell'anagrafica e la creazione del documento in formato PDF che è trasmesso in modalità sicura alla piattaforma di firma grafometrica per la creazione della sottoscrizione.
Le applicazioni Allianz Bank provvedono inoltre alla archiviazione gestionale delle immagini dei documenti sottoscritti (rendering) e all'invio al Cliente via e-mail della copia di quanto sottoscritto.

5.3.3 Piattaforma di firma grafometrica

La postazione del Financial Advisor e le applicazioni Allianz Bank colloquiano con la piattaforma di firma grafometrica installata presso il data center InfoCert che svolge le seguenti operazioni:

- Raccolta dati biometrici rilevati dal dispositivo;
- Cifratura dei dati biometrici;
- Inserimento sicuro dei dati nel contratto;
- Firma digitale del documento a chiusura del processo di firma grafometrica;
- Marcatura temporale del documento a validazione dell'istante di firma;
- Creazione della immagine rendering del documento firmato per la restituzione alle applicazioni Allianz Bank;
- Invio del documento firmato con firma grafometrica al sistema di Conservazione.

La piattaforma di firma grafometrica è integrata con i servizi di certificazione e conservazione erogati dalla Certification Authority InfoCert.

A chiusura del processo di firma grafometrica del documento, grazie al servizio di firma digitale automatica InfoCert, Allianz Bank appone la firma digitale di uno o più suoi procuratori attraverso una procedura automatica, a presidio dell'integrità del documento e dei dati biometrici crittografati.
Sui documenti firmati è apposta una marca temporale utilizzando il servizio InfoCert.
Le marche temporali emesse da InfoCert hanno una validità di 20 anni, ovvero il maggior tempo di conservazione della marca stessa eventualmente concordato con il cliente.

I documenti firmati con firma grafometrica sono inviati al sistema di conservazione InfoCert, per la garanzia dell'inalterabilità, la leggibilità e la disponibilità nel tempo dei documenti informatici.

6 Controllo del sistema di sottoscrizione

Sono predisposte procedure e sistemi automatici per il controllo dello stato dell'intera infrastruttura tecnica deputata all'erogazione dei servizi di firma grafometrica.

6.1 Strumenti per il controllo del sistema

Presso il data-center InfoCert sono installati strumenti di controllo automatico che consentono di controllare il sistema valutando gli eventi e gli stati in cui il sistema stesso viene a trovarsi.
Il sistema è configurato in modo da intraprendere, in funzione dell'evoluzione dei suoi stati, delle azioni fra le seguenti tipologie:

- memorizzazione degli eventi;
- riconoscimento di eventi;
- risoluzione dei problemi;
- notificazione agli operatori.

6.2 Verifiche di sicurezza e qualità

Le procedure operative e le procedure di sicurezza di InfoCert sono soggette a controlli periodici legati sia alla verifiche ispettive per il conseguimento ed il successivo mantenimento delle certificazioni dei Sistemi di Gestione (Sistema di Gestione della Qualità ISO 9001, Sistema di Gestione della Sicurezza delle Informazioni ISO 27001, Sistema di Gestione dei Servizi Informatici ISO 20000) sia a verifiche predisposte dalla funzione di auditing interno.
I controlli mirano a verificare la corretta applicazione delle procedure previste e la loro effettiva funzionalità in relazione agli obiettivi prefissati.
Oltre alle attività di auditing di processi sono pianificate le analisi e i controlli da effettuare sulle registrazioni prodotte dalle applicazioni e dai sistemi durante il normale funzionamento. Tale attività ha lo scopo di controllare che tutti gli eventi verificatisi rientrino nella normale operatività e che non si verifichino eventi pregiudicanti la sicurezza.
La registrazione e la conseguente imputabilità degli eventi verificatisi costituiscono inoltre una valida misura di sicurezza.

7 Misure di sicurezza

Il sistema di firma elettronica avanzata in modalità grafometrica è protetto da numerose misure di sicurezza poste a presidio dei dati del Cliente e dei documenti sottoscritti. Le misure di sicurezza sviluppate da Allianz Bank per la protezione delle postazioni di lavoro dei Financial Advisors, sono completate dalle misure di sicurezza InfoCert, poste a protezione del data-center da cui sono erogati i servizi di firma elettronica.

7.1 Misure di sicurezza InfoCert

InfoCert ha realizzato un sistema di sicurezza del data-center da cui eroga i servizi di firma elettronica che minimizza tutti i rischi derivanti dal malfunzionamento dei sistemi,della rete e delle applicazioni, oltre che dall'intercettazione non autorizzata o dalla modifica dei dati.
Il sistema di sicurezza sviluppato è articolato su tre livelli:

- Sicurezza fisica, per la sicurezza degli ambienti da cui sono erogati i servizi;
- Sicurezza delle procedure, che cura gli aspetti prettamente organizzativi;
- Sicurezza logica, tramite la predisposizione di misure hardware e software che affrontano i problemi e i rischi connessi con la tipologia del servizio, con l'infrastruttura utilizzata e garantiscono l'affidabilità della rete.

7.1.1 Sicurezza fisica

Le misure adottate forniscono adeguate garanzie di sicurezza in merito a:

- Caratteristiche dell'edificio e della costruzione;
- Sistemi anti-intrusione attivi e passivi;
- Controllo degli accessi fisici;
- Alimentazione elettrica e condizionamento dell'aria;
- Protezione contro gli incendi;
- Protezione contro gli allagamenti;
- Modalità di archiviazione dei dati;
- Siti di archiviazione dei dati.

7.1.2 Sicurezza delle procedure

A garanzia che nessun individuo possa singolarmente compromettere o alterare la sicurezza globale del sistema oppure svolgere attività non autorizzate nella gestione del sistema di firma elettronica avanzata, la gestione operativa del sistema è affidata a persone diverse con compiti separati e ben definiti.
Il personale addetto alla progettazione ed erogazione del servizio di certificazione è stato selezionato in base alla esperienza nella progettazione, realizzazione e conduzione di servizi informatici e a caratteristiche di affidabilità e riservatezza. Sono pianificati periodici interventi di formazione per sviluppare la consapevolezza dei compiti assegnati e fornire ogni competenza (tecnica, organizzativa e procedurale) necessaria a svolgere i compiti assegnati.

7.1.3 Sicurezza logica

Per garantire la sicurezza dei dati e delle operazioni, tutto il software utilizzato realizza le seguenti funzioni di sicurezza:

- Identificazione e autenticazione degli utenti e dei processi che richiedono di operare nel sistema;
- Controllo accessi;
- Imputabilità ed audit di ogni evento riguardante la sicurezza;
- Gestione delle risorse di memorizzazione volta ad impedire la possibilità di risalire alle informazioni in precedenza contenute o registrate da altri utenti;
- Autodiagnostica ed integrità dei dati e del software (controllo allineamento tra le copie operative e quelle di riferimento, controllo della configurazione del software, protezione dai virus);
- Configurazione hardware e software per garantire la continuità del servizio.

InfoCert utilizza per il servizio di firma elettronica avanzata un'infrastruttura di sicurezza della rete basata sull'uso di meccanismi che realizzino un canale sicuro tra le postazioni di raccolta dei dati biometrici e l'infrastruttura software di gestione dei dispositivi.
Il sistema è supportato da specifici prodotti di sicurezza (anti intrusione di rete, monitoraggio, protezione da virus, firewall) e da tutte le relative procedure di gestione e aggiornamento.

8 Cessazione del servizio

Il servizio di firma elettronica avanzata può essere interrotto per revoca del consenso da parte del Cliente o per dismissione del servizio da parte di Allianz Bank. Si illustrano di seguito gli effetti dei due casi di cessazione.

8.1 Revoca del consenso da parte del cliente

In caso il Cliente scelga di revocare il proprio consenso all'utilizzo del servizio di FEA, secondo la procedura descritta al paragrafo seguente, dal momento della revoca i documenti che regolano i rapporti tra il Cliente e Allianz Bank saranno sottoscritti mediante firma autografa su carta. e/o modalità equivalente Restano salvi i documenti precedentemente sottoscritti con firma elettronica avanzata in modalità grafometrica.

8.1.1 Procedura per la revoca del consenso

La revoca del consenso deve essere esercitata mediante la compilazione di un apposito Modulo di Revoca. Il Modulo è disponibile presso il Financial Advisor di riferimento e viene firmato in modalità grafometrica.

8.2 Dismissione del servizio FEA

Qualora Allianz Bank decidesse di dismettere il servizio di FEA, i documenti che regolano i rapporti tra il Cliente ed Allianz Bank saranno sottoscritti mediante firma autografa su carta e/o modalità equivalente.
Restano salvi i documenti precedentemente sottoscritti con firma elettronica avanzata in modalità grafometrica, che continueranno ad essere conservati a norma da Allianz Bank per tutto il termine di conservazione previsto.
Allianz Bank continuerà a conservare inoltre il Modulo di Attivazione e la copia del documento di identità del Cliente fino alla scadenza del termine ventennale di conservazione previsto dal **DPCM** per il Soggetto Erogatore.

9 Contatti

9.1 Contatto per assistenza

Qualora necessario, i Clienti che necessitino di assistenza, informazioni aggiuntive sul servizio di firma elettronica e cessazione del servizio possono rivolgersi al proprio Financial Advisor o direttamente ad Allianz Bank (i contatti sono indicati sul sito Allianz Bank[7].)

9.2 Procedura di richiesta dei documenti

Rivolgendosi ad Allianz Bank il Cliente può ottenere copia di tutta la documentazione relativa al servizio di firma elettronica avanzata o con questa sottoscritta.
I documenti in oggetto sono forniti all'indirizzo e-mail dichiarato sotto forma di copia per immagine (*rendering*), non contenente i dati biometrici all'interno per ragioni di sicurezza. Tali documenti hanno la stessa efficacia probatoria dell'originale conservato negli archivi Allianz Bank fino a quando la loro conformità non è espressamente disconosciuta, ai sensi dell'articolo 23-bis comma 2 del **CAD**.

Esclusivamente ai fini di produzione in giudizio o di esibizione di fronte alla Pubblica Autorità, il Cliente può chiedere all'Intermediario l'esibizione della documentazione **in originale**. I documenti sono duplicati informatici contenenti i dati biometrici e corredati dalle evidenze informatiche di corretta conservazione[8] prodotti da InfoCert.

[7] http://www.allianzbank.it/servizio-clienti
[8] File in formato XML contenenti le impronte di hash dei documenti conservati, firmati digitalmente dal Responsabile della Conservazione e marcati temporalmente.