Manuale Operativo sui documenti firmati con Firma Elettronica Avanzata "FirmaSmart" (Strong Customer Authentication)

Allianz Bank
Financial Advisors

Vers. 2 del Settembre 2022

ABK0045-RK0045_01/2022

ABK0046-RK0046_01/2022

1 Introduzione al documento

1.1 Scopo e campo di applicazione

Il presente documento è il Manuale dei processi di formazione e conservazione elettronica dei documenti firmati con firma elettronica avanzata (di seguito anche "Manuale") ai sensi della Deliberazione CNIPA 11/2004.

Il Manuale risponde alla necessità di documentare il processo di creazione, sottoscrizione e conservazione di documenti informatici, effettuato con le modalità di cui agli articoli 3 e 4 della sopraccitata deliberazione, nonché le procedure di sicurezza e di tracciabilità dei documenti conservati.

1.2 Riferimenti Normativi e tecnici

1) Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito referenziato come "Reg. eIDAS".

2) 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.

3) 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".

4) 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".

5) Determinazione AgID n. 121/2019 recante - Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate.".

6) Decreto Legislativo 30 giugno 2003, n. 196 (GU n. 174 del 29 luglio 2003) – Codice per la protezione dei dati personali e successive modificazioni anche ai sensi del Regolamento Ue 679 del 4 maggio 2016 ed operativo a partire dal 25 maggio 2018 ("GDPR").

7) Decreto Legislativo n.231 del 21 novembre 2007 (GU n.290 del 14 dicembre 2007) e s.m.i. – "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 del 30 luglio 2019 – Provvedimento recante Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo la, 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) DPCM 3 dicembre 2013 (GU n.59 del 12-3-2014 - Suppl. Ordinario n. 20) - 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.

1.1 Termini e 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.

ARCHIVIAZIONE	è il processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo. È passo propedeutico alla conservazione, per il quale non sono previsti particolari obblighi di legge.
CONSERVAZIONE/ CONSERVAZIONE SOSTITUTIVA O A NORMA	il processo che consente di conservare i documenti in modalità informatica a norma di legge e che risponde a quanto stabilito nella deliberazione CNIPA 11 del 19 febbraio 2004.

DOCUMENTO ANALOGICO ORIGINALE	documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;
DOCUMENTO INFORMATICO	la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
DATI SENSIBILI	ai sensi dell'articolo 4, comma 1, lettera d) del Decreto Legislativo 30 giugno 2003, n.196, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale
EVIDENZA INFORMATICA	una 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. 3, comma 1, lett. 10, Reg. eIDAS);
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. 3, comma 1, lett. 12, Reg. eIDAS)
FIRMA ELETTRONICA AVANZATA	insieme di dati in firma 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 (art. 3, comma 1, lett. 11, Reg. eIDAS)

ABK0046-RK0046_01/2022

FIRMA GRAFOMETRICA	applicazione pratica che consiste nella apposizione di una firma autografa con uno speciale pennino, su un tablet che procede alla rilevazione del movimento, della pressione esercitata e dall'andatura della mano e, in genere di una serie di caratteristiche idonee a permettere l'identificazione certa della sottoscrizione
FIRMA SCA	un particolare tipo di firma elettronica avanzata ottenuta grazie al riconoscimento del soggetto firmatario (o Cliente) mediante una transazione SCA, la cui conferma abilita l'apposizione del sigillo contenente le informazioni della SCA sul documento
TRANSAZIONE SCA	La SCA si realizza in presenza di almeno due dei seguenti tre fattori: 1) Fattore di conoscenza: qualcosa che solo il cliente sa (password, PIN ecc.); 2) Fattore di possesso: qualcosa che solo il cliente ha (smartphone, token bancario ecc.); 3) Fattore di inerenza: qualcosa che solo il cliente è (riconoscimento facciale, impronta digitale ecc.).
TRANSAZIONE SCA DI TIPO SECURE CALL	Transazione SCA mediante la quale il cliente effettua o riceve una chiamata dal/sul proprio numero telefonico certificato con il soggetto erogatore e inserisce tramite toni DTMF un codice OTP (one time password)
TRANSAZIONE SCA DI TIPO SOFTWARE TOKEN	Transazione SCA che si declina in due modalità operative: 1) Ricezione di una notifica push sul cellulare certificato e riconoscimento del cliente mediante PIN o dati biometrici (o inserimento diretto degli stessi nel caso si operi direttamente dal dispositivo mobile) 2) Scansione di un QR Code e generazione dallo stesso di un codice univoco da inserire poi a conferma dell'operazione di firma
IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI (o HASH)	la sequenza dei simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima 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)

ABK0046-RK0046_01/2022

LOTTO DI DOCUMENTI	insieme di documenti raggruppati secondo un criterio di aggregazione, aventi un file indice (file di chiusura del lotto) che attesta la conservazione con l'apposizione della firma del Responsabile della Conservazione e della marca temporale.
MARCA TEMPORALE	il riferimento temporale che consente la validazione temporale, così come definita all'art. 1 comma 1 lettera i) DPCM del 30 marzo 2009. La marca temporale è opponibile ai terzi.
PDF (PORTABLE DOCUMENT FORMAT)	formato di file creato da Adobe Systems nel 1993 per lo scambio di documenti. Il PDF è un formato a schema fisso basato su un linguaggio di descrizione di pagina che permette di rappresentare documenti in modo indipendente dall'hardware, dal software e dal sistema operativo; ogni PDF incapsula una descrizione completa del documento, che include testo, caratteri, immagini e grafica. PDF è uno standard aperto
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
RESPONSABILE DELLA CONSERVAZIONE	il soggetto cui sono attribuite funzioni, adempimenti, attività e responsabilità relative al processo di conservazione ottica sostitutiva conformemente a quanto previsto all'art. 5 della deliberazione Cnipa 11 del 19 febbraio 2004.
RIFERIMENTO TEMPORALE	informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici, così come definito all'art. 1 comma 1 lettera m) DPCM del 30 marzo 2009.
HARDWARE SECURITY MODULE	dispositivo crittografico ad alte prestazioni utilizzato per apporre automaticamente la firma digitale e la validazione temporale ad elevati volumi di documenti informatici
POSTA ELETTRONICA CERTIFICATA	sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici

EXTENSIBLE MARKUP LANGUAGE	linguaggio derivato dall'SGML (Standard Generalized Markup Language), metalinguaggio che permette di creare altri linguaggi. Mentre l'HTML è un'istanza specifica dell'SGML, XML costituisce a sua volta un metalinguaggio, più semplice dell'SGML, largamente utilizzato per la descrizione di documenti sul Web. L'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati. Tali strutture vengono definite utilizzando dei marcatori (markup tags). Diversamente dall'HTML, l'XML consente all'utente di definire marcatori personalizzati, dandogli il controllo completo sulla struttura di un documento. Si possono definire liberamente anche gli attributi dei singoli marcatori.

1.2 Acronimi

CA	Certification Authority
CF	Consulente Finanziario abilitato all'offerta fuori sede
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione (ora DigitPA)
D. LGS	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
FEA	Firma Elettronica Avanzata
GU	Gazzetta Ufficiale della Repubblica Italiana
HSM	Hardware Security Module
PDF	Portable Document Format
PEC	Posta Elettronica Certificata
SCA	Strong Customer Authentication
SG	Sistema di Gestione
SGD	Sistema di Gestione Documentale
SSL	Secure Socket Layer
TSA	Time Stamping Authority
TSS	Time Stamping Service
TU	Testo Unico
URL	Uniform Resource Locator
XML	Extensible Markup Language

1.3 Attori coinvolti nel processo di firma

In questo capitolo sono individuati i differenti soggetti che intervengono a vario titolo nelle diverse fasi del processo di creazione dei documenti elettronici, digitalizzazione dei documenti cartacei, datacertazione e conservazione elettronica documentale.

Soggetto Erogatore → Allianz Bank Financial Advisors S.p.A.

Soggetto Realizzatore → Accenture Financial Advanced Solutions & Technology

Soggetto Conservatore → Infocert S.p.A.

Soggetto sottoscrittore → Cliente

Soggetto Erogatore	Allianz Bank Financial Advisors S.p.A. è il Soggetto Erogatore della soluzione di FEA come definito dall'articolo 55 comma 2 lettera a) del DPCM. 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 FEA. L'identificazione certa del sottoscrittore del documento è eseguita per Allianz Bank Financial Advisors S.p.A. (di seguito definita solo come Allianz Bank) dai propri Consulenti Finanziari abilitati all'offerta fuori sede (di seguito definiti solo come Consulenti Finanziari) presenti sul territorio, nel rispetto della procedura di identificazione definita a validata da Allianz Bank, nella quale viene richiesta la presenza fisica del sottoscrittore. 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 così come modificato dal D.Lgs 125/2019 (7) sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente. Ai sensi dell'articolo 57 comma 2 del DPCM Allianz Bank ha stipulato una idonea copertura assicurativa per la responsabilità civile, nel rispetto dei massimali previsti dal DPCM. Nello svolgimento delle proprie attività di Soggetto Erogatore, si avvale sul territorio di Consulenti Finanziari, che si occupano di, nel rispetto del DPCM: • identificare l'utente sottoscrittore; • raccogliere copia del documento di identità dello stesso utente sottoscrittore; I Consulenti Finanziari sono attivati dal Soggetto Erogatore a seguito di un adeguato addestramento.

Soggetto Realizzatore	Accenture Financial Advanced Solutions & Technology 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 SCA grazie alla propria piattaforma. Il Soggetto Realizzatore è tenuto a garantire che: a) la soluzione di firma SCA sviluppata sia conforme alle specifiche tecniche e funzionali definite con il soggetto erogatore b) la soluzione tecnologica sviluppata consenta la connessione univoca della firma al sottoscrittore e garantisca il controllo esclusivo del sottoscrittore del sistema di generazione della firma, ivi inclusi i codici identificativi inoltrati al Cliente per l'autorizzazione dell'operazione; c) La soluzione tecnologica sviluppata per la firma SCA utilizzi adeguate tecniche di cifratura dei dati trattati, al fine di impedirne la visualizzazione "in chiaro"; d) Il documento informatico non possa subire modifiche dopo l'apposizione della firma.

Soggetto Conservatore	Infocert è il soggetto conservatore nella soluzione FEA adottata da Allianz Bank. InfoCert svolge il ruolo di Responsabile della Conservazione dei documenti in base all'atto di affidamento a questo scopo sottoscritto da Allianz Bank, per la delega dei compiti e delle responsabilità ad InfoCert come soggetto terzo dotato di adeguata competenza ed esperienza, ai sensi dell'art. 6, comma 6 del DPCM 3 dicembre 2013. Il Soggetto Conservatore svolge le seguenti attività: • definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente; • gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente; • genera il rapporto di versamento, secondo le modalità previste dal manuale di conservazione; • genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione di Infocert; • effettua il monitoraggio della corretta funzionalità del sistema di conservazione; • assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi; • al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; • adotta analoghe misure con riguardo all'obsolescenza dei formati; • provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione; • adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12 del DPCM 3 dicembre 2013; • assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;

ABK0046-RK0046_01/2022

	• assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza; • provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti; • predispone il manuale di conservazione di cui all'art. 8 del DPCM 3 dicembre 2013 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.
Soggetto Sottoscrittore	Il soggetto sottoscrittore è il Cliente che sottoscrive la documentazione contrattuale avvalendosi delle firme elettroniche (firma SCA). Il sottoscrittore è tenuto a garantire: • la correttezza e la completezza dei dati personali forniti al soggetto erogatore, incluso il corretto recapito telefonico per utilizzo della firma SCA; • di aver preso visione della documentazione descrittiva del servizio FEA prima dell'adesione al servizio, presente nella sezione c.d. FirmaSmart dell'area riservata di Internet Banking della Banca.

2. Processo di firma

2.1 La firma elettronica avanzata

La "firma elettronica avanzata" (FEA) è stata introdotta nel nostro ordinamento dal decreto legislativo 30 dicembre 2010, n. 235 di modifica del CAD ed è oggi definita dall'art. 3, comma1, n. 11 del Reg. eIDAS come una firma elettronica che soddisfi i requisiti enunciati nell'art. 26, ossia:

a) *è connessa unicamente al firmatario;*
b) *è idonea a identificare il firmatario;*
c) *è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;*
d) *è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.*

Dal punto di vista probatorio, il medesimo decreto legislativo n. 235/2010, così come modificato dal D.Lgs 26 agosto 2016, n. 179, ha inoltre stabilito, integrando l'art. 20 del CAD, che:

"Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida".

Per poter sostanziare nella pratica una 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 e delle Linee Guide emanate dall'AgID ai sensi dell'art. 71 CAD.

La firma SCA è un particolare tipo di firma elettronica che consente al Cliente di apporre le proprie firme su documenti elettronici tramite l'utilizzo del cellulare/smartphone del sottoscrittore. L'accettazione delle clausole di firma avviene mediante conferma con transazione SCA; il riconoscimento del sottoscrittore, secondo i dettami regolamentari, l'invio del token per accedere al documento e l'audit log delle operazioni eseguite assicurano il rispetto dei requisiti di Firma Elettronica Avanzata. Questo documento evidenzia le regole generali e le procedure seguite dal Soggetto Erogatore Allianz Bank per l'erogazione e l'utilizzo del servizio di Firma Elettronica Avanzata con SCA.

2.2 Operatività per firma SCA

L'intero processo web segue organicamente i seguenti step:

1) Attivazione/Disattivazione del servizio;
2) Firma proposta;
3) Rifiuto proposta;
4) Consultazione documenti firmati

L'applicazione presente nella sezione FirmaSmart dei propri canali digitali (Internet Banking o App Mobile) permette al cliente di:

1. Attivare e disattivare il servizio
2. Visionare le proposte d'investimento inviategli dal proprio Consulente Finanziario (previa condivisione nell'incontro di consulenza finanziaria)
3. Firmare le proposte con meccanismi di firma elettronica avanzata
4. Rifiutare le proposte non di interesse *(in alternativa al punto 3. di cui sopra)*
5. Consultare l'archivio delle proposte firmate

2.2.1 Attivazione del servizio

Il processo di identificazione del soggetto firmatario e di sua adesione a questa modalità di firma è eseguito una-tantum al primo utilizzo del servizio di firma SCA e si compone delle seguenti attività:

1) Lettura delle note informative esposte in pagina
2) Accettazione delle note tramite transazione SCA

2.2.2 Firma della proposta

Dopo l'adesione al servizio di firma elettronica SCA, il processo di sottoscrizione dei prodotti, e le eventuali successive operazioni (versamenti aggiuntivi, switch/passaggi tra fondi, rimborsi/liquidazioni), prevede le seguenti attività:

il Consulente Finanziario imposta, attraverso gli strumento ed i sistemi informativi che gli vengono messi a disposizione da Allianz Bank, le operazioni finanziarie che costituiranno la proposta commerciale e che verranno sottoposte nella loro interezza alla verifica di adeguatezza rispetto al profilo di rischio del cliente, come richiesto dalla normativa MiFID, dopodiché consolida ed invia online gli ordini al cliente.

Tale proposta è firmata digitalmente da Allianz Bank per garantirne la provenienza e l'integrità del documento

Il cliente visiona le proposte finanziarie attive nella sezione FirmaSmart presente nei propri canali digitali (Internet Banking o App Mobile) e a seguito della pressione del tasto "*Prosegui*" autorizza la proposta (previa visione del contratto stesso in formato PDF), confermando l'operazione con una transazione SCA per ogni "*gruppo d'ordine*" (insiemi di operazioni). Il cliente in questa fase ha anche la facoltà di eseguire i download del documento/i. Tali documenti possono essere altresì salvati su supporto duraturo del cliente, visualizzati e stampati.

Più nel dettaglio: in caso di più operazioni contenute nella medesima proposta, le stesse verranno visionate dal cliente nei relativi moduli in formato PDF e firmate per ogni singolo modulo. Saranno confermate, e quindi considerate accolte e processabili da Allianz Bank, esclusivamente le proposte completamente autorizzate con sottoscrizione di tutti i moduli contenuti nella proposta stessa. Non saranno altresì recepite né confermate al cliente le proposte autorizzate parzialmente. Solo al termine del processo di firma di tutti i moduli viene data conferma al cliente in Internet Home Banking che la proposta è "*confermata*".
La proposta per taluni prodotti d'investimento (tipicamente le c.d. "sottoscrizioni iniziali") può prevedere più sottoscrittori intestatari, che quindi dovranno autorizzare le operazioni contenute nei relativi contratti, ed in questo caso, ognuno dei sottoscrittori dovrà firmare i moduli nella propria Internet Home Banking, sempre mediante transazione SCA. Solo quando tutti i sottoscrittori abbiano autorizzato tutte le operazioni la proposta verrà dichiarata al cliente come "confermata".
Le regole ed i controlli sull'applicabilità della FirmaSmart vengono gestite a monte, nella fase di costituzione della proposta nell'applicativo (One) della Banca in uso al Consulente Finanziario.

Da parte del cliente la conferma dell'operazione di autorizzazione è possibile solo a fronte della lettura completa del contratto/i d'ordine e l'esplicita presa visione delle note.

Il sistema appone un sigillo nel contratto che riporta i parametri che identificano l'operazione e il soggetto sottoscrittore legandoli univocamente al documento che si sta firmando e rendendolo di fatto immodificabile mediante una firma qualificata. I dati contenuti nel sigillo sono opportunamente cifrati, al fine di impedirne la visualizzazione "in chiaro";

L'utilizzo della SCA all'interno del processo autorizzativo di apposizione del sigillo garantisce l'autenticità dell'operazione secondo gli standard di sicurezza già in uso presso Allianz Bank.

Il timestamp contenuto nel sigillo certifica l'ora esatta in cui è avvenuta l'operazione.
Il token SCA utilizzato nella fase di approvazione lega l'operazione autorizzativa al documento stesso e al sistema di generazione della firma su cui il Cliente ha pieno controllo.

Il documento/i firmato viene inviato in Conservazione Sostitutiva a norma presso l'ente certificatore Infocert, ed archiviato nel sistema documentale della Banca, per poter essere visionato dal Cliente in ogni momento, mediante la consultazione dell'archivio delle proposte

ABK0046-RK0046_01/2022

firmate. Inoltre il documento/i viene inviato al sistema "Arco" della Banca e storicizzato per consultazione successiva anche a parte del Consulente Finanziario.

Durata della proposta: il cliente ha facoltà di visualizzare e poter firmare/rifiutare la proposta finanziaria nella propria Internet Home Banking entro un massimo di quindici giorni di calendario dalla creazione della stessa da parte del Consulente Finanziario, dopodiché la proposta cessa di essere valida. Dal sedicesimo giorno la proposta non è più disponibile per il cliente ed assume lo stato di "scaduta" nei sistemi della Banca.

2.2.3 Rifiuto della proposta

Il cliente visiona le proposte finanziarie attive nella sezione FirmaSmart presente nei propri canali digitali (Internet Banking o App Mobile) ed in alternativa alla conferma di cui al punto sopra riportato, può scegliere di respingere la proposta mediante pressione del link "*Rifiuta proposta*" e quindi procedere con il rifiuto della proposta stessa (eventualmente anche avendone letto in dettaglio il contenuto) confermando l'operazione sempre mediante una transazione SCA.

3 Componenti tecnologiche utilizzate

La soluzione tecnologica utilizzata per il processo di firma elettronica avanzata (FEA) si compone dei macro-elementi elencati qui di seguito e descritti nella tabella che segue:

- postazione del Consulente Finanziario;
- cellulare/smartphone del Cliente;
- applicazione Allianz Bank di creazione del documento (One);
- piattaforma di firma SCA del Soggetto Realizzatore;
- piattaforma di archiviazione conservativa del Soggetto Conservatore.

Postazione del Consulente Finanziario	La postazione del Consulente Finanziario coincide con il proprio PC e/o con il tablet (iPad) utilizzato per l'operatività
Cellulare/smartphone del cliente	Il cellulare/smartphone del Cliente è lo strumento certificato in fase di adesione al servizio di firma SCA ed abilitato a ricevere le notifiche nel caso di Software Token o ad effettuare le chiamate nel caso di Secure Call (oppure ricevere le chiamate nel caso di Secure Call con cliente all'estero, giacché si tratta di numero verde altrimenti non raggiungibile da fuori Italia). La corretta immissione identifica il Cliente firmatario e lo abilita alla sottoscrizione del documento.
Applicazione One	Servizio informativo di Allianz Bank attraverso il quale i Consulenti Finanziari possono censire nuovi clienti, ricercare quelli già in portafoglio, consultarne i dati anagrafici e patrimoniali e, tra le altre funzionalità, creare le proposte finanziarie, verificarne l'adeguatezza secondo il profilo di rischio, sceglierne la modalità di firma da parte del cliente e quindi inviarle all'Internet Home Banking in caso di applicabilità della FirmaSmart, nonché poi seguirne il tracking delle operazioni.
Piattaforma di firma SCA del soggetto Realizzatore	La piattaforma di firma SCA messa a disposizione dal soggetto realizzatore che svolge le seguenti principali attività: • creazione e verifica della transazione SCA; • inserimento sicuro dei dati nel contratto; • apposizione di due firme digitali appartenenti ad Allianz Bank; • salvataggio nel documentale e invio in conservazione sostitutiva del documento firmato • invio di copia flat ai sistemi informativi per consultazione da parte del Consulente Finanziario

ABK0046-RK0046_01/2022

Piattaforma di archiviazione conservativa del soggetto Conservatore	La piattaforma di conservazione della documentazione messa a disposizione da Infocert che effettua la conservazione a norma dei documenti come previsto dalla normativa vigente (per la durata di venti anni).

4 Controllo del sistema di sottoscrizione

Sono predisposte procedure e/o sistemi automatici per il controllo dello stato dell'intera infrastruttura tecnica deputata all'erogazione dei servizi di firma avanzata mediante SCA

4.1 Strumenti per il controllo del sistema

Presso il data center del Soggetto Realizzatore 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.

4.2 Verifiche di sicurezza e qualità

Le procedure operative e le procedure di sicurezza del Soggetto Realizzatore sono soggette a controlli periodici legati sia alle 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) che 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.

5 Controllo del sistema di conservazione

Sono predisposte procedure e/o sistemi automatici per il controllo dello stato dell'intera infrastruttura tecnica deputata all'erogazione dei servizi per la conservazione a norma della documentazione sottoscritta.

5.1 Strumenti per il controllo del sistema

Presso il data center del Soggetto Conservatore 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.

5.2 Verifiche di sicurezza e qualità

Le procedure operative e le procedure di sicurezza del Soggetto Conservatore sono soggette a controlli periodici legati sia alle 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) che 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.

6 Misure di sicurezza

Il sistema di firma elettronica avanzata in modalità SCA 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 Consulenti Finanziari, sia fisse che in mobilità, sono completate dalle misure di sicurezza del Soggetto Realizzatore e del Soggetto Conservatore, poste a protezione del data-center da cui sono erogati i servizi di firma elettronica.

6.1 Misure di sicurezza del Soggetto Realizzatore

Il Soggetto Realizzatore ha predisposto 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.

Il Soggetto Realizzatore utilizza per il servizio di firma elettronica un'infrastruttura di sicurezza della rete basata sull'uso di meccanismi che realizzino un canale sicuro tra le postazioni di raccolta dei dati 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.

6.2 Misure di sicurezza del Soggetto Conservatore

Il Soggetto Conservatore ha predisposto un sistema di sicurezza del data-center da cui eroga i servizi di conservazione 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.

Il Soggetto Conservatore per il servizio di conservazione è supportato da specifici prodotti e sistemi
di sicurezza (anti-intrusione di rete, monitoraggio, protezione da virus, firewall) e da tutte le relative procedure di gestione e aggiornamento.

7 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.

7.1 Revoca del consenso da parte del Cliente

Il cliente può disporre la revoca del servizio facendone richiesta alla Banca.

7.1.1 Procedura per la revoca del consenso

Per disporre la revoca del servizio il Cliente può agire attraverso il proprio Internet Home Banking, mediante transazione SCA analogamente a quanto fatto per l'attivazione del servizio stesso, nella sezione c.d. FirmaSmart, oppure con comunicazione sottoscritta in forma cartacea da inviarsi ad Allianz Bank Financial Advisors S.p.A, piazza Tre Torri n.3 - 20145 – Milano.

7.2 Dismissione del servizio FEA

La Banca si riserva di poter dismettere il servizio in oggetto. 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, 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. dandone preventiva comunicazione ai Clienti, nelle modalità previste dalla normativa vigente.

8 Contatti e Assistenza

Modalità e procedura per assistenza

per qualsiasi richiesta di chiarimento relativa al servizio è possibile rivolgersi al Servizio Assistenza Clienti:

- al numero +39.02.55.50.61.32, oppure
- scrivere una mail all'indirizzo customer.center@allianzbank.it ,
- oppure attraverso corrispondenza all'indirizzo: Allianz Bank Financial Advisors S.p.A., Piazza Tre Torri 3, 20145 Milano.

8.1 Procedura di richiesta dei documenti

La documentazione sottoscritta dal cliente, potrà essere richiesta dal cliente alla Banca in ogni momento, attraverso i contatti e le modalità di cui al punto sopra.