Firma Elettronica Avanzata Grafometrica e OTP

Documento riassuntivo delle caratteristiche tecniche del Servizio

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 Documento Unico Consensi e dichiarazioni (di seguito anche "**UNICO**") e rappresenta il documento riassuntivo delle caratteristiche tecniche del servizio di firma elettronica.

1.2 Riferimenti normativi e tecnici

Riferimenti normativi

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 5bis, 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 di firma elettronica	• un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I (art. 3, comma 1, lett. 15, **Reg. eIDAS**)
certificato di firma elettronica	• un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona (art. 3, comma 1, lett. 14, Reg. eIDAS);
Certificatore [Certification Authority]	• il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime
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**).

Matrix	• L'applicativo Allianz erogato dal data-center della Compagnia e messo a disposizione degli Intermediari per la gestione del proprio portafoglio, sotto l'aspetto commerciale, contabile, amministrativo, anagrafico e di monitoraggio. Consente la gestione di trattative commerciali, l'inserimento di soluzioni assicurative proposte alla Clientela, l'inserimento dei dati anagrafici del Cliente, la creazione di documenti da sottoporre alla firma del Cliente, da inviare alla casella mail del Cliente e da archiviare. • Matrix provvede inoltre alla trasformazione delle firme sottoscritte all'interno del documento in formato immagine (rendering), all'archiviazione gestionale dei documenti con immagini di firma dei documenti sottoscritti (rendering), all'invio al Cliente via e-mail della copia di quanto sottoscritto qualora ne abbia rilasciato il consenso e alla trasmissione dei documenti sottoscritti per Conservazione a Norma.
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 qualificata basata su un su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo 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	• Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare (art. 3, comma 1, lett. 10, **Reg. eIDAS**);
Firma elettronica avanzata	• Una firma elettronica che soddisfi i requisiti di cui all'articolo 26 (art. 3, comma 1, lett. 11, **Reg. eIDAS**)
Firma elettronica qualificata	• Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche (art. 3, comma 1, lett. 12, **Reg. eIDAS**)
Firma Grafometrica	• un particolare tipo di firma elettronica ottenuta grazie al rilevamento dinamico dei dati biometrici (ritmo, pressione, velocità, accelerazione, movimento aereo, ecc.) della firma di un individuo tramite una penna elettronica su specifici dispositivi idonei a rilevare le caratteristiche sopra indicate
Firma OTP	• un particolare tipo di firma elettronica (One Time Password) ottenuta grazie al riconoscimento del soggetto firmatario (o Cliente) mediante l'invio di un codice identificativo sul suo cellulare, la cui successiva immissione a sistema certifica l'apposizione della firma del cliente mediante appositi *click* nei punti firma previsti dal documento.
Folder	• un sistema centralizzato in cui Allianz archivia la documentazione relativa alle polizze ed ai clienti

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
Numero di cellulare	• numero di cellulare abilitato alla ricezione del codice OTP mediante SMS
Tablet (iPad)	• tablet (iPad) o pc dotati di connettività che consentono di visualizzare direttamente il documento e raccogliere la firma del Cliente e i parametri biometrici connessi, nel caso di firma grafometrica
XML	• Extensible Markup Language, metalinguaggio utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati.
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**)
validazione temporale elettronica	• dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento
Modulo Unico consensi e dichiarazioni / Modulo UNICO	• documento contrattuale elaborato da Allianz 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 Compagnia

1.4 Attori coinvolti nel processo di firma

Gli attori coinvolti nel processo di firma elettronica avanzata (FEA) sono elencati qui di seguito e descritti nella tabella che segue.

Soggetto Erogatore	Allianz ed Intermediari Allianz
Soggetto Realizzatore	Namirial S.P.A
Soggetto Conservatore	Infocert S.P.A.
Soggetto Sottoscrittore	Cliente

Soggetto Erogatore	Allianz 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 dai propri Intermediari presenti sul territorio [1], nel rispetto della procedura di identificazione definita a validata da Allianz, ed è 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 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 Intermediari (di seguito definiti anche solo come "**Intermediari**"), che si occupano di, nel rispetto del DPCM:
	• identificare l'utente sottoscrittore; • raccogliere copia del documento di identità dello stesso utente sottoscrittore; • raccogliere la sottoscrizione dell'utente sulla dichiarazione di adesione al servizio di firma grafometrica e/o al servizio di firma OTP, mediante il modulo UNICO, per accettazione delle condizioni del servizio da parte dell'utente medesimo; • supporto al sottoscrittore nell'apposizione della firma, nella fornitura e revoca del consenso. Gli Intermediari sono attivati dal Soggetto Erogatore a seguito di un adeguato addestramento. Per il dettaglio degli Intermediari abilitati si rimanda al tool di ricerca disponibile sul portale Allianz[2].

[1] Si rimanda al portale Allianz (http://www.allianz.it/contatti-servizi/contatta-consulente) per il dettaglio geografico della rete di Intermediari

[2] http://www.allianz.it/contatti-servizi/contatta-consulente

Soggetto Realizzatore	Namirial S.p.A. 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 e OTP grazie alla propria piattaforma. Namirial è una società IT di software e servizi ed è un Qualified Trust Service Provider che fornisce Trust Services come Firme Elettroniche, Firme Elettroniche Avanzate (Grafometriche e con Strong Authentication), Firme Elettroniche Qualificate (anche Digitali), Posta Elettronica Certificata, Fatturazione Elettronica e Conservazione Sostitutiva a più di 500.000 utenti. I gruppi di utenti serviti da Namirial si articolano in diversi settori, tra cui: Ordini Professionali di cui fanno parte Medici, Avvocati, Ingegneri, Consulenti del Lavoro, Dottori Commercialisti, Strutture Cooperative e Imprenditoriali tra cui la Media e Piccola Impresa, la Pubblica Amministrazione, i Trasporti, le Banche e le Assicurazioni e le aziende di classe enterprise. La sede principale è a Senigallia con ulteriori uffici in Italia e sedi in Austria e Romania, da cui vengono serviti utenti situati in tutta l'Europa, gli Stati Uniti, il Medio Oriente e l'Africa. Per maggiori informazioni si rimanda al sito www.namirial.com Il Soggetto Realizzatore è tenuto a garantire che: a) la soluzione di firma (grafometrica o OTP) sviluppata sia conforme alle specifiche tecniche e funzionali definite con Allianz; 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 dati biometrici di generazione della firma ed i codici identificativi inoltrati al Cliente tramite SMS; c) La soluzione tecnologica sviluppata per la firma grafometrica utilizzi adeguate tecniche di cifratura dei dati biometrici raccolti e 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. 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 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; • 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 grafometrica oppure firma OTP). Il sottoscrittore è tenuto a garantire: • la correttezza e la completezza dei dati personali forniti al soggetto erogatore (Allianz o Intermediari Allianz), incluso il corretto recapito telefonico per utilizzo della firma OTP; • la consegna all'Intermediario o incaricato Allianz di un documento di identità in corso di validità al momento della sottoscrizione del documento UNICO; • di aver preso visione della documentazione descrittiva del servizio FEA prima dell'adesione al servizio.

2 Processo di firma

2.1 Premessa

La fattispecie "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, comma 1, 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*"[3].
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**.

In questo contesto si inseriscono le **due tipologie di firma FEA, la firma grafometrica e di firma OTP** (One Time Password) descritte nel presente manuale.

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

La **firma grafometrica** è un particolare tipo di firma elettronica che si ottiene dal rilevamento dinamico dei dati biometrici (ritmo, pressione, velocità, accelerazione, movimento aereo, ecc.) della firma di un individuo tramite una penna elettronica.
La firma grafometrica viene apposta tramite l'utilizzo di specifici strumenti, 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, secondo i dettami regolamentari, deve assicurare il rispetto dei requisiti per la validità della firma elettronica avanzata.

La **firma OTP** è un particolare tipo di firma elettronica che consente al Cliente di apporre le proprie firme su documenti elettronici tramite l'utilizzo del cellulare del sottoscrittore. L'accettazione delle clausole di firma avviene semplicemente cliccando sui relativi campi firma (click2sign); 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 (nel prosieguo semplicemente indicato come Allianz) per l'erogazione e l'utilizzo del servizio di Firma Elettronica Avanzata in modalità grafometrica e in modalità OTP.

2.2 Operatività per firma grafometrica

2.2.1 Fase 1: adesione al 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 elettronica e si concretizza nelle seguenti attività:

1. l'Intermediario raccoglie il documento di identità del sottoscrittore e ne verifica le informazioni;
2. l'Intermediario acquisisce copia per immagine del documento di identità utilizzando uno scanner ovvero la fotocamera del device mobile;
3. Matrix genera il Modulo UNICO in PDF che viene passato al servizio di firma grafometrica di Namirial e visualizzato al Cliente;
4. il Cliente è invitato a leggere su monitor o tablet (iPad) il Modulo UNICO e sottoscriverlo mediante firma grafometrica;
5. il servizio di firma grafometrica di Namirial raccoglie i dati biometrici e li inserisce cifrati all'interno del Modulo UNICO in PDF;

6. il processo prevede l'apposizione al Modulo UNICO di due firme digitali automatiche appartenenti a soggetti Allianz e di una marca temporale. Il Modulo UNICO sottoscritto è successivamente inviato a Matrix e salvato con le immagini di firma nel sistema di archiviazione di Allianz unitamente alla copia del documento di identità;
7. Matrix, qualora il Cliente abbia rilasciato apposito consenso, invia alla casella elettronica indicata dal Cliente un file in formato PDF contenente l'immagine del documento sottoscritto. Su richiesta del Cliente, l'Intermediario stamperà eventualmente una copia cartacea del Modulo UNICO;
8. Matrix invia il Modulo UNICO sottoscritto e la copia del documento di identità al sistema di Conservazione Elettronica a Norma di Infocert per i 20 anni previsti dall'articolo 57 comma 1 lettera b) del **DPCM**.

Come dettagliato dal Modulo UNICO, tutte le variazioni ai dati e alle informazioni, nonché ai consensi forniti, devono essere effettuate compilando e sottoscrivendo un nuovo Modulo UNICO.

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

2.2.2 Fase 2: firma del documento (polizza)

Dopo l'adesione al servizio di firma grafometrica, il processo di sottoscrizione di un documento prevede le seguenti attività:

1. L'Intermediario incontra il cliente e si accerta della corretta identità del cliente identificandolo attraverso un documento di riconoscimento in corso di validità;
2. l'Intermediario accede a Matrix attraverso il proprio web browser o attraverso la app installata sul tablet (iPad) ed elabora la proposta commerciale per il Cliente che salva in Matrix;
3. l'Intermediario, in accordo con il Cliente, seleziona la funzione che permette di firmare il documento in modalità grafometrica;
4. Matrix genera il documento in formato PDF che viene passato al servizio di firma grafometrica di Namirial e visualizzato sul monitor o sul tablet (iPad);
5. il Cliente prende visione del contratto in tutte le sue parti e successivamente appone la propria firma sul pad (tavoletta) o sul tablet (iPad) utilizzando l'apposito pennino elettronico e conferma;
6. L'Intermediario appone la propria firma sui punti previsti dalla documentazione in modo del tutto analogo a quanto effettuato dal Cliente;
7. il pad o il tablet (iPad) registrano i parametri biometrici associati alla firma ovvero:
   - velocità orizzontale di scorrimento della penna (asse x)

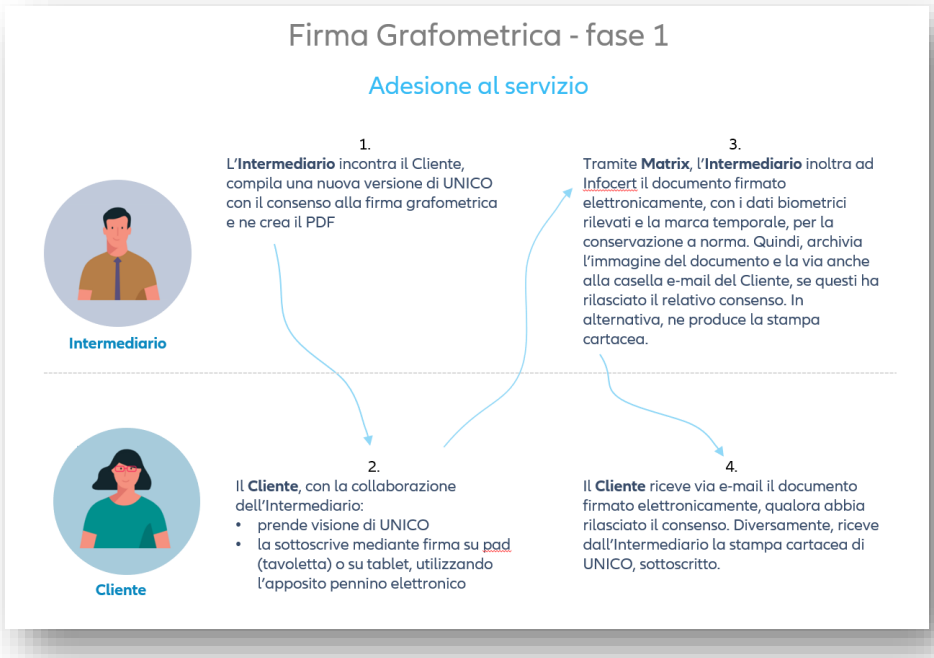
- velocità verticale di scorrimento della penna (asse y)
- posizione del pennino sull'asse orizzontale (asse x)
- posizione del pennino sull'asse verticale (asse y)
- pressione esercitata
- accelerazione del pennino
- tempo di firma

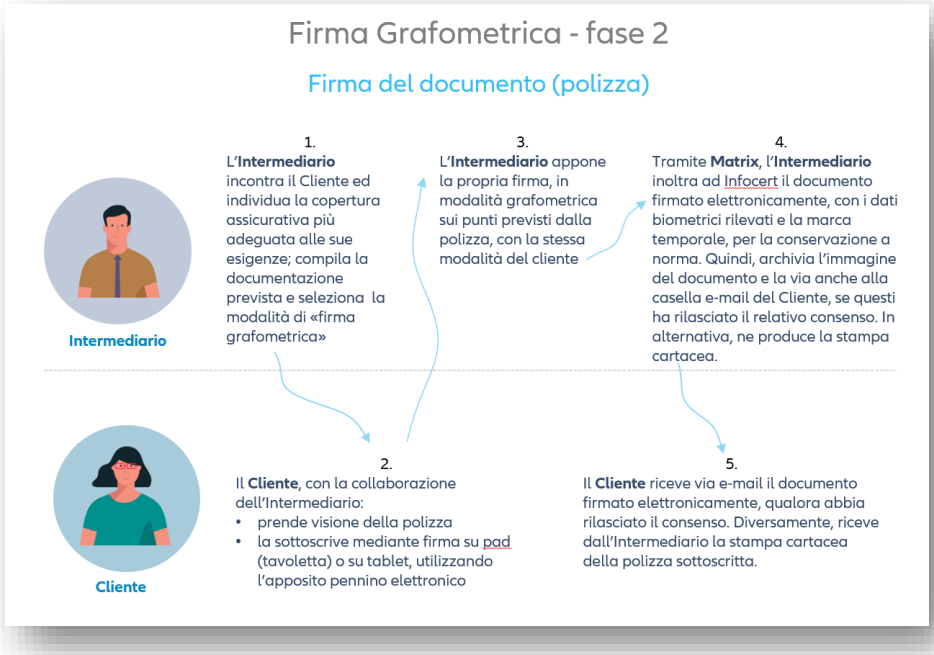
8. Il servizio di firma grafometrica di Namirial quindi:
   - raccoglie e crittografa i dati biometrici raccolti e li inserisce nel documento PDF;
   - inserisce i dati crittografati nel documento PDF insieme a una serie di codici che garantiscono l'immodificabilità del documento nel tempo e l'impossibilità di estrarre i dati biometrici stessi dal PDF per riutilizzarli su un altro documento;
   - appone sul documento, in automatico, due firme digitali di soggetti appartenenti ad Allianz;
   - appone sul documento una marca temporale emessa dalla TSA (Time Stamping Authority) di Namirial;
   - invia il documento al sistema di conservazione elettronica a norma di Infocert;
   - restituisce a Matrix un file in formato PDF contenente l'immagine del documento sottoscritto e della sottoscrizione apposta;
9. Matrix riceve, dal servizio di firma grafometrica di Namirial, il documento sottoscritto, lo archivia trasformando le firme apposte dal cliente in immagini e, qualora il Cliente abbia rilasciato apposito consenso, invia alla casella email indicata dal Cliente nel Modulo UNICO copia del documento con le firme apposte trasformate in immagini;
10. Matrix invia il documento sottoscritto al sistema di Conservazione Elettronica a Norma di Infocert per i 20 anni previsti dall'articolo 57 comma 1 lettera b) del **DPCM**.

Oltre alla polizza, con questa stessa esperienza d'uso, il Cliente potrà sottoscrivere altra tipologia di documentazione mediante firma grafometrica.

2.2.3 Flow sintetico del processo

Il processo di firma grafometrica viene qui di seguito sintetizzato nelle fasi dettagliate nei due precedenti paragrafi.





2.3 Operatività per firma OTP

2.3.1 Fase 1: adesione al 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 OTP e si compone delle seguenti attività:

1. l'Intermediario richiede al Cliente quanto segue:
    - il documento di identità: ne verifica le informazioni, ne acquisisce copia per immagine (a mezzo scanner o fotocamera del device mobile) che archivia in Matrix;
    - il numero di cellulare: deve essere associato in modo univoco al Cliente stesso;
    - casella email;
    - consensi: consenso alla firma della documentazione contrattuale mediante OTP e consenso alla ricezione della documentazione contrattuale sulla casella mail fornita all'Intermediario;
2. l'Intermediario, tramite Matrix, genera il Modulo UNICO e lo inoltra alla casella mail del Cliente affinché possa essere visionato prima della sottoscrizione;
3. l'Intermediario, qualora il Cliente desideri procedere con il suo censimento in Matrix, avvia la richiesta di creazione del codice OTP al servizio di Namirial – cliccando sui punti firma – che si concretizza nell'inoltro di un SMS al numero di cellulare del Cliente contenente il codice OTP.
4. il Cliente riceve sul suo cellulare il codice OTP che viene immesso in un'apposita schermata di Matrix attivando il servizio di firma OTP di Namirial che controlla la corrispondenza dell'OTP inserito in Matrix con quello inoltrato via SMS al Cliente. Se esiste corrispondenza, quindi il Cliente è stato correttamente identificato, si può proseguire. Diversamente, l'Intermediario dovrà richiedere la creazione di un nuovo codice OTP (vedi punto 3.);
5. Il servizio di firma OTP di Namirial appone sul documento la marca temporale e le due firme digitali di soggetti appartenenti ad Allianz. Infine, restituisce a Matrix il file pdf contenente l'immagine del documento sottoscritto;
6. Matrix riceve il pdf del documento sottoscritto e ne:
    - inoltra copia alla casella mail del Cliente. Su richiesta del Cliente, l'Intermediario stamperà eventualmente una copia cartacea del documento;
    - archivia copia con immagini di firma in Folder;
    - inoltra copia del Modulo UNICO, unitamente all'Audit Trail delle operazioni effettuate, a Infocert per la conservazione a norma per i 20 anni previsti dall'articolo 57 comma 1 lettera b) del **DPCM.**
7. l'Intermediario stamperà, eventualmente su richiesta del Cliente, una copia cartacea del Modulo UNICO;

Come dettagliato dal Modulo UNICO, tutte le variazioni ai dati e alle informazioni, nonché ai consensi forniti, devono essere effettuate compilando nuovamente e sottoscrivendo il Modulo UNICO.

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

2.3.2 Fase 2: firma del documento (polizza)

Dopo l'adesione al servizio di firma elettronica OTP, il processo di sottoscrizione della polizza prevede le seguenti attività:

1. il Cliente, in collaborazione con l'Intermediario, valuta le possibili soluzioni assicurative (garanzie, opzioni da attivare, clausole…) ed individua la tipologia di polizza che soddisfa le proprie esigenze;
2. l'Intermediario, tramite Matrix, inoltra alla casella e-mail del Cliente:
   a) la documentazione precontrattuale come prevista da IDD (DIP, DIP aggiuntivo, Condizioni di assicurazione, allegato 3 e 4 del regolamento IVASS n. 40/2018);
   b) il riepilogo dei bisogni e delle esigenze del Cliente;
   c) la proposta di polizza; affinché possa prenderne visione prima della sottoscrizione dei documenti di cui al punto sub b) e sub c). Matrix archivia la documentazione inoltrata al Cliente;
3. l'Intermediario avvia la fase di presa visione e sottoscrizione della polizza e del Riepilogo dei bisogni ed esigenze assicurative del Cliente che consiste nella visualizzazione al Cliente della documentazione e nella successiva immissione di *click* sui punti firma. I punti firma previsti per l'Intermediario saranno valorizzati in automatico da Matrix;
4. l'Intermediario, tramite il Front End di Namirial, avvia la richiesta di creazione del codice OTP che si concretizza nell'inoltro di un SMS al numero di cellulare del Cliente contenente il codice OTP.
5. il Cliente riceve sul suo cellulare il codice OTP che viene immesso in un'apposita schermata di Namirial (se in mobilità digitato sull'iPad dell'Intermediario) attivandone il servizio di firma OTP che controlla la corrispondenza dell'OTP inserito in Matrix con quello inoltrato via SMS al Cliente. Se esiste corrispondenza, quindi il Cliente è stato correttamente identificato, la polizza da sottoscrivere viene firmata, diversamente l'Intermediario dovrà richiedere la creazione di un nuovo codice OTP (vedi punto 4.);
6. dopo la sottoscrizione del documento il servizio di firma OTP di Namirial:
   - appone, per ciascun punto firma del Cliente, cognome e nome dello stesso e la marca temporale prodotta dalla TSA (Time Stamping Authority) di Namirial;
   - appone due firme digitali di soggetti appartenenti ad Allianz;

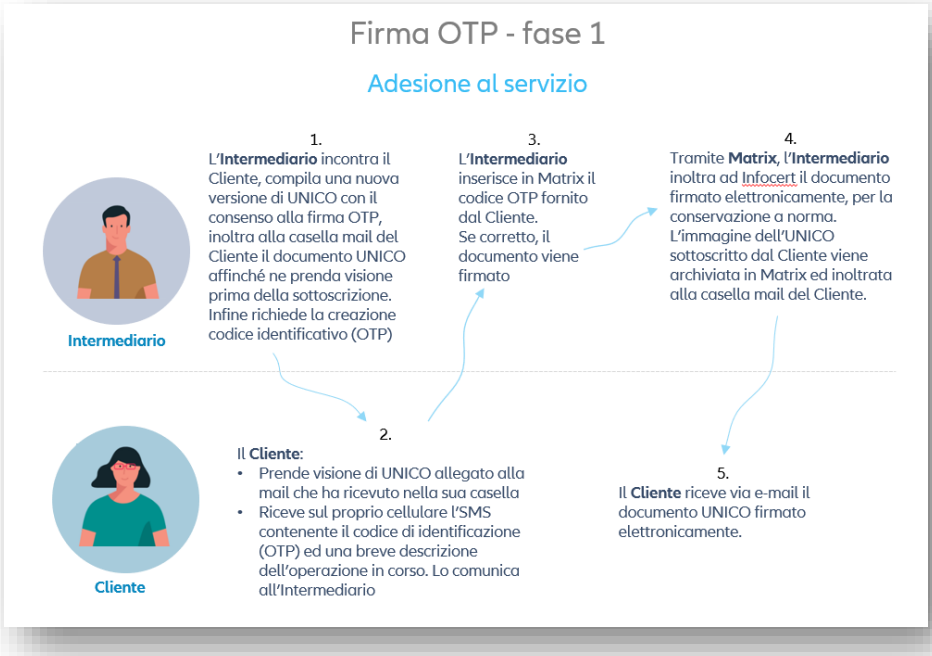
- restituisce a Matrix un file in formato PDF contenente il documento sottoscritto dal cliente;

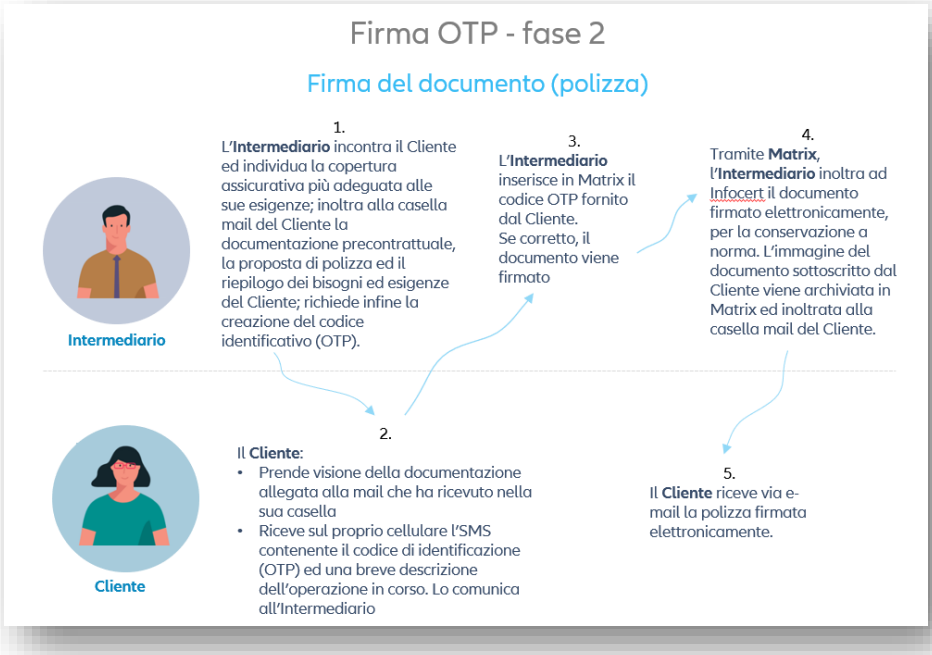
7. Matrix riceve il pdf del documento sottoscritto e quindi:
   - inoltra copia alla casella mail del Cliente. Su richiesta del Cliente, l'Intermediario stamperà eventualmente una copia cartacea del documento;
   - archivia copia con immagini di firma in Folder;
   - inoltra copia della documentazione sottoscritta, unitamente all'Audit Trail delle operazioni effettuate, a Infocert per la conservazione a norma per i 20 anni previsti dall'articolo 57 comma 1 lettera b) del **DPCM.**
8. L'Intermediario stamperà, eventualmente su richiesta del Cliente, una copia cartacea della documentazione sottoscritta.

Oltre alla polizza, con questa stessa esperienza d'uso, il Cliente potrà sottoscrivere altra tipologia di documentazione mediante firma OTP.

2.3.4 Flow sintetico del processo

Il processo di firma OTP viene qui di seguito sintetizzato nelle fasi dettagliate nei due precedenti paragrafi.





2.3.5 Fase 2: firma del documento (polizza) con modalità OTP 2.0

La modalità di firma OTP 2.0 prevede l'invio, da parte dell'Intermediario, di una mail alla casella di posta del Cliente contenente un link per procedere con la sottoscrizione della polizza in autonomia tramite dispositivo personale del Cliente. Questa modalità non prevede ulteriori consensi da raccogliere, ma usa gli stessi consensi prestati per la modalità OTP tradizionale.

Dopo l'adesione al servizio di firma elettronica OTP, il processo di sottoscrizione della polizza con modalità OTP 2.0 prevede le seguenti attività:

1. il Cliente, in collaborazione con l'Intermediario, valuta le possibili soluzioni assicurative (garanzie, opzioni da attivare, clausole…) ed individua la tipologia di polizza che soddisfa le proprie esigenze;
2. l'Intermediario, tramite Matrix, inoltra alla casella e-mail del Cliente:
   a) la documentazione precontrattuale come prevista da IDD (DIP, DIP aggiuntivo, Condizioni di assicurazione, allegato 3 e 4 del regolamento IVASS n. 40/2018);
   b) il riepilogo dei bisogni e delle esigenze del Cliente;
   c) la proposta di polizza; affinché possa prenderne visione prima della sottoscrizione dei documenti di cui al punto sub b) e sub c). Matrix archivia la documentazione inoltrata al Cliente;
   d) il link per accedere al portale Allianz per procedere alla sottoscrizione dei documenti.
3. Il Cliente, premendo sul link di cui al punto precedente, ingaggia Namirial sul cui Front End avvia la fase di presa visione e sottoscrizione della polizza e del Riepilogo dei bisogni ed esigenze assicurative del Cliente che consiste nella visualizzazione della documentazione e nella successiva immissione di *click* sui punti firma. I punti firma previsti per l'Intermediario saranno valorizzati in automatico dalla procedura;
4. Il Cliente, tramite Namirial, avvia la richiesta di creazione del codice OTP che si concretizza nell'inoltro di un SMS al proprio numero di cellulare contenente il codice OTP.
5. il Cliente riceve sul suo cellulare il codice OTP che viene immesso in un'apposita schermata di Namirial attivandone il servizio di firma OTP che controlla la corrispondenza dell'OTP inserito con quello inoltrato via SMS al Cliente. Se esiste corrispondenza, quindi il Cliente è stato correttamente identificato, la polizza da sottoscrivere viene firmata, diversamente il Cliente dovrà richiedere la creazione di un nuovo codice OTP (vedi punto 4.);
6. dopo la sottoscrizione del documento il servizio di firma OTP di Namirial:
   - appone, per ciascun punto firma del Cliente, cognome e nome dello stesso e la marca temporale prodotta dalla TSA (Time Stamping Authority) di Namirial;
   - appone due firme digitali di soggetti appartenenti ad Allianz;

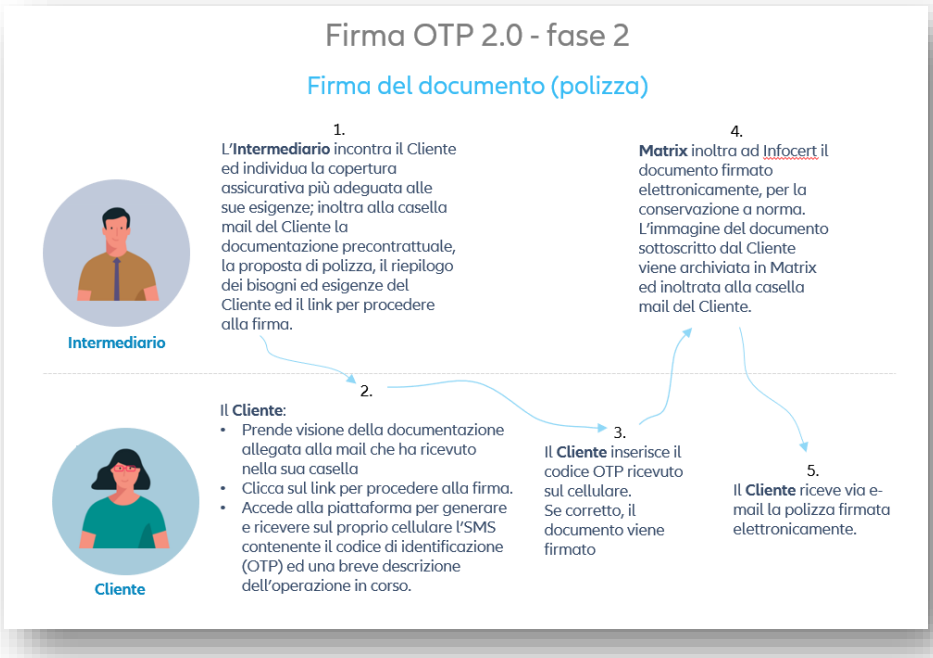
- restituisce a Matrix un file in formato PDF contenente il documento sottoscritto dal cliente;

7. Matrix riceve il pdf del documento sottoscritto e quindi:
   - inoltra copia alla casella mail del Cliente. Su richiesta del Cliente, l'Intermediario stamperà eventualmente una copia cartacea del documento;
   - archivia copia con immagini di firma in Folder;
   - inoltra copia della documentazione sottoscritta, unitamente all'Audit Trail delle operazioni effettuate, a Infocert per la conservazione a norma per i 20 anni previsti dall'articolo 57 comma 1 lettera b) del **DPCM.**
8. L'Intermediario stamperà, eventualmente su richiesta del Cliente, una copia cartacea della documentazione sottoscritta.

Oltre alla polizza, con questa stessa esperienza d'uso, il Cliente potrà sottoscrivere altra tipologia di documentazione mediante firma OTP.

2.3.6 Flow sintetico del processo

Il processo di firma OTP 2.0 viene qui di seguito sintetizzato nelle fasi dettagliate nel precedente paragrafo.



3 Soluzione tecnologica utilizzata

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 dell'Intermediario;
- cellulare del Cliente;
- applicazioni Allianz di creazione del documento (Matrix);
- piattaforma di firma (grafometrica o OTP) del Soggetto Realizzatore;
- piattaforma di archiviazione conservativa del soggetto Conservatore.

Postazione dell'Intermediario	La postazione dell'Intermediario coincide con il proprio PC e/o con il tablet (iPad) utilizzato per l'operatività, allestito per poter raccogliere la firma elettronica avanzata. La soluzione tecnologica prescelta per la firma grafometrica utilizza dispositivi hardware dotati di tecnologia *touch* in grado di rilevare i principali parametri della firma dell'utente (posizione, pressione, velocità, accelerazione, tempo). I dispositivi utilizzati possono afferire a due categorie: • pad di firma: dispositivi per postazione fissa, collegati a mezzo cavo USB al PC dell'Intermediario. Il documento è visualizzato al Cliente su un secondo monitor ovvero, se le dimensioni del pad lo consentono, direttamente sul dispositivo. • Dispositivi mobili: tablet (iPad), pc dotati di connettività che consentono di visualizzare direttamente il documento e raccogliere la firma del Cliente e i parametri biometrici connessi[4].
Cellulare del Cliente (solo per firma OTP)	Il cellulare del Cliente è lo strumento certificato in fase di adesione al servizio di firma OTP ed abilitato a ricevere, mediante SMS, il codice da inserire in Matrix. La corretta immissione identifica il Cliente firmatario e lo abilita alla sottoscrizione del documento.
Applicazioni Allianz	L'applicazione Allianz coinvolta è Matrix, come descritta nel paragrafo 1.3 Definizioni.
Piattaforma di firma grafometrica del soggetto Realizzatore (Namirial S.P.A.)	La postazione dell'Intermediario e Matrix colloquiano con la piattaforma di firma grafometrica erogata da Namirial che svolge le seguenti principali attività: • raccolta dati biometrici rilevati dal dispositivo; • cifratura dei dati biometrici; • inserimento sicuro dei dati nel contratto; • apposizione a chiusura del processo di firma grafometrica, in automatico, di due firme digitali di soggetti appartenenti ad Allianz; • marcatura temporale del documento a validazione dell'istante di firma; • restituzione del documento firmato alle applicazioni Allianz.

[4] In caso di utilizzo del dispositivo Apple Ipad ® non è raccolto l'indice di pressione.

Piattaforma di firma OTP del soggetto Realizzatore (Namirial S.P.A.)	La postazione dell'Intermediario e Matrix colloquiano con la piattaforma di firma OTP erogata da Namirial che svolge le seguenti principali attività: • creazione e verifica dei codici OTP; • inserimento sicuro dei dati nel contratto; • apposizione a chiusura del processo di firma OTP, in automatico, di due firme digitali di soggetti appartenenti ad Allianz; • marcatura temporale del documento a validazione dell'istante di firma; • restituzione del documento firmato alle applicazioni Allianz.
Piattaforma di archiviazione conservativa del soggetto Conservatore (Infocert S.P.A.)	Matrix colloquia con la piattaforma di conservazione della documentazione di Infocert che effettua conservazione a norma (documenti firmati) e sostitutiva (carta d'identità), come previsto dalla normativa vigente.

4 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 e OTP.

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 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 grafometrica ed in modalità OTP 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 per la protezione delle postazioni di lavoro degli Intermediari, 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.

6.1.1 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.

6.1.2 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, 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.

6.1.3 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.

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 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.

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.

6.2.1 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.

6.2.2 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, 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 archiviazione e conservazione 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.

6.2.3 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.

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. Si illustrano di seguito gli effetti dei due casi di cessazione.

7.1 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 le società saranno sottoscritti mediante firma autografa su carta, firma elettronica qualificata o firma digitale.
Restano salvi i documenti precedentemente sottoscritti con firma elettronica avanzata in modalità grafometrica o OTP.

7.1.1 Procedura per la revoca del consenso

La revoca del consenso deve essere esercitata mediante la compilazione di un nuovo Modulo UNICO consensi e dichiarazioni, che va a sostituire integralmente il modulo precedentemente sottoscritto. Il Modulo è disponibile presso l'Intermediario di riferimento.

7.2 Dismissione del servizio FEA

Qualora Allianz decidesse di dismettere il servizio di FEA, i documenti che regolano i rapporti tra il Cliente e le società saranno sottoscritti mediante firma autografa su carta e/o modalità equivalente. Restano salvi i documenti precedentemente sottoscritti con firma elettronica avanzata in modalità grafometrica o OTP, che continueranno ad essere conservati a norma da Allianz per tutto il termine di conservazione previsto.

Allianz continuerà inoltre a conservare il Modulo UNICO consensi e dichiarazioni e la copia del documento di identità del Cliente fino alla scadenza del termine ventennale di conservazione previsto dal **DPCM** per il Soggetto Erogatore.

8 Contatti

8.1 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 Intermediario.

8.2 Procedura di richiesta dei documenti

Rivolgendosi all'Intermediario il Cliente può ottenere copia di tutta la documentazione relativa al servizio di firma elettronica avanzata o con questa sottoscritta.
In particolare, è possibile ottenere uno o più documenti in formato PDF contenenti l'immagine di:

- il Modello UNICO consensi e dichiarazioni sottoscritto all'adesione al servizio;
- la copia del documento di identità raccolto al momento dell'adesione al servizio;
- i documenti sottoscritti con la firma grafometrica o con la firma OTP.

I documenti in oggetto sono forniti all'indirizzo e-mail dichiarato sotto forma di copia per immagine (*rendering)*. Tali documenti hanno la stessa efficacia probatoria dell'originale conservato negli archivi Allianz fino a quando la loro conformità non è espressamente disconosciuta, ai sensi dell'articolo 23-bis comma 2 del **CAD**.

In caso di necessità, esclusivamente ai fini di produzione in giudizio o esibizione di fronte alla Pubblica Autorità, il Cliente può chiedere all'Intermediario l'esibizione della documentazione **in originale**. I documenti sono forniti all'indirizzo e-mail dichiarato e sono duplicati informatici contenenti i dati biometrici e, nel caso di firma OTP, l'audit trail delle operazioni effettuate, corredati dalle evidenze informatiche di corretta conservazione[5] prodotti dal Soggetto Realizzatore.

[5] File in formato XML contenenti le impronte di hash dei documenti conservati, firmati digitalmente dal Responsabile della Conservazione e marcati temporalmente.