Firma Elettronica Avanzata in modalità Grafometrica

Documento riassuntivo delle caratteristiche tecniche del Servizio

ridefiniamo / gli standard

Sommario

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

1.2 Riferimenti normativi e tecnici

Riferimenti normativi

1) Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (GU n. 42 del 20 febbraio 2001) – Testounico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
2) Decreto Legislativo 7 marzo 2005, n. 82 (GU n. 112 del 16 maggio 2005) – Codice dell'Amministrazione Digitale e successive modifiche e integrazioni, di seguito referenziato come "**CAD".**
3) Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 (GU n.117 del 21 maggio 2013) – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71, di seguito referenziato come "**DPCM".**
4) Deliberazione CNIPA numero 45/2009 (GU n. 282 del 3 dicembre 2009) – Regole per il riconoscimento e la verifica del documento informatico.
5) Determinazione Commissariale DigitPA N. 69/2010 (GU n. 191 del 17 agosto 2010) – Modifiche alla Deliberazione 21 maggio 2009 n. 45 del Centro Nazionale per l'Informatica nella pubblica Amministrazione, recante "Regole per il riconoscimento e la verifica del documento informatico".
6) Decreto Legislativo 30 giugno 2003, n. 196 (GU n. 174 del 29 luglio 2003) – Codice per la protezione dei dati personali.
7) Decreto Legislativo n.231 del 21 novembre 2007 (GU n.290 del 14 dicembre 2007) – "Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione".
8) Ufficio Italiano Cambi: parere del 14 giugno 2001.
9) Provvedimento di Banca d'Italia del 11 aprile 2013 – Provvedimento recante disposizioni attuative in materia di adeguata verifica della clientela, ai sensi dell'art. 7, comma 2, del Decreto Legislativo 21 novembre 2007, n. 231.
10) Deliberazione CNIPA n. 11 del 19 febbraio 2004 (GU n. 57 del 9 marzo 2004) – Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo

a garantire la conformità dei documenti agli originali - Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

11) 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.

1.3 Definizioni

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

Certificato Qualificato	• il certificato elettronico conforme ai requisiti di cui all'allegato I della Direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva (art 1, comma 1 lettera f **CAD**)

Certificato, Certificato Digitale	• Insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica.
	• Nel certificato compaiono altre informazioni tra cui:
	  ○ il Certificatore che lo ha emesso;
	  ○ il periodo di tempo in cui il certificato può essere utilizzato;
	  ○ altri campi (estensioni) che determinano caratteristiche aggiuntive al certificato.

Certificatore [Certification Authority]	• il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime (art 1, comma 1 lettera g **CAD**)
Chiave privata	• l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico. (art 1, comma 1 lettera h **CAD**). • Nei processi di cifratura di dati è l'elemento segreto che serve a decifrare i dati cifrati.
Chiave pubblica	• l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche (art 1, comma 1 lettera i **CAD**). • Nei processi di cifratura di dati è l'elemento inserito nel sistema che è utilizzato per i dati raccolti, ad esempio i dati biometrici connessi alla firma grafometrica.
Conservazione / Conservazione a norma	• Processo di archiviazione sicura a lungo termine di documenti informatici o copie per immagine di documenti analogici, che ne assicura l'integrità, la sicurezza, l'immodificabilità, la disponibilità e il mantenimento del valore legale
Copia informatica di documento informatico	• Il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari (art 1, comma 1 lettera i-quater **CAD**).

Copia per immagine di documento analogico	• Il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto (art 1, comma 1 lettera i-ter **CAD**).
Duplicato informatico	• Il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario (art 1, comma 1 lettera i-quinquies **CAD**).
Evidenza informatica	• Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (articolo 1, co. 1, lettera f **DPCM**)
Firma digitale	• Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (art 1, comma 1 lettera s **CAD**)
Firma elettronica	• L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (art 1, comma 1 lettera q **CAD**)
Firma elettronica avanzata	• Insieme di dati in forma elettronica allegati oppure connessi a un documenti informatico che consentono l'identificazione del sottoscrittore del documento e garantiscono la connessione univoca al sottoscrittore, creati con mezzi sui quali il sottoscrittore può conservare il controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art 1, comma 1 lettera q-bis **CAD**)
Firma elettronica qualificata	• Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art 1, comma 1 lettera r **CAD**)
Firma Grafometrica	• un particolare tipo di firma elettronica ottenuta grazie al rilevamento dinamico dei dati calligrafici (ritmo, pressione, velocità, inclinazione della penna, movimento, ecc.) della firma di un individuo tramite una penna elettronica su specifici dispositivi idonei a rilevare le caratteristiche sopra indicate
Hash / impronta	• la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione a una evidenza informatica di una opportuna funzione di hash (articolo 1, co. 1, lettera h **DPCM**)
Funzione di hash	• una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguale a partire da evidenze informatiche differenti (articolo 1, co. 1, lettera g **DPCM**)
Marca temporale (Time Stamp Token)	• il riferimento temporale che consente la validazione temporale (articolo 1, co. 1, lettera i **DPCM**)
Modulo Anagraico consensi e dichiarazioni / Modulo Anagrafico	• documento contrattuale elaborato da AXA 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

Pad di firma	• dispositivi per postazione fissa, collegati a mezzo cavo USB a un PC, con cui si raccolgono i dati biometrici
PDF/A	• standard internazionale (ISO 19005-1), sottoinsieme dello standard PDF, appositamente pensato per l'archiviazione nel lungo periodo di documenti elettronici in quanto garantisce che il documento sia visualizzabile sempre allo stesso modo, anche a distanza di tempo e con programmi software diversi
Rendering	• copia informatica di documento informatico con contenuto e forma uguali a quello del documento di partenza, che non contiene gli elementi biometrici, di firma digitale o di marca temporale
Responsabile della Conservazione	• soggetto responsabile del sistema di conservazione dei documenti
Tablet	• tablet pc dotati di connettività che consentono di visualizzare direttamente il documento e raccogliere la firma del cliente e i parametri biometrici connessi
XML	• Extensible Markup Language, metalinguaggio utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati.

2 Generalità (Inquadramento normativo)

La fattispecie "firma elettronica avanzata" (FEA) è stata introdotta nel nostro ordinamento dal D. Lgsn. 235/2010, mediante il quale, modificando parzialmente il CAD, ha inserito una nuova definizione alla lettera q-bis) dell'art. 1: la FEA è definita come: l'"insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del sottoscrittore del documento e garantiscono la connessione univoca al sottoscrittore, creati con mezzi sui quali il sottoscrittore può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati".
Dal punto di vista probatorio, il medesimo D. Lgs n. 235/2010 ha inoltre stabilito, integrando l'art. 21 del CAD, che:
"Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile[1].

L'adozione di FEA, è subordinata al rispetto delle regole tecniche di cui al DPCM 22 febbraio 2013 pubblicato nella Gazzetta Ufficiale n. 117 del 21 maggio 2013.

Nel descritto contesto normativo, si inserisce la firma grafometrica, un particolare tipo di firma elettronica che si ottiene dal rilevamento dinamico dei dati calligrafici (ritmo, pressione, velocità, inclinazione della penna, movimento, ecc.) della firma di un individuo tramite una penna elettronica.
La firma grafometrica viene apposta tramite l'utilizzo di specifici "tablet", idonei a rilevare le caratteristiche 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 consentire di assicurare il rispetto dei requisiti per la validità della firma elettronica avanzata.

Il presente documento intende rappresentare i principi, le regole generali e le procedure seguite dal Soggetto Erogatore AXA Assicurazioni S.p.A. (nel proseguo semplicemente indicato come AXA) per l'erogazione e l'utilizzo del servizio di Firma Elettronica Avanzata in modalità grafometrica.

2.1 Attori

2.1.1 Soggetto Erogatore

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

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

2.1.2 Agenti AXA

AXA, nello svolgimento delle proprie attività di Soggetto Erogatore, si avvale sul territorio di intermediari iscritti alla Sez. A) del Registro Unificato (.R.U.I) di cui al Codice delle Assicurazioni D.Lgs. 209/2005 ed al Reg. n. 5 emanato da ISVAP (di seguito definiti anche solo come "**Agenti**"), i quali , nell'espletamento della funzione, e, nel rispetto del DPCM:

- Identificano l'utente sottoscrittore ;
- raccolgono copia del documento di identità dello stesso utente sottoscrittore;
- raccolgono la sottoscrizione dell'utente sulla dichiarazione di adesione al servizio di Firma Grafometrica (DAC) per accettazione delle condizioni del servizio da parte dell'utente medesimo;
- assistonoil sottoscrittore nell'apposizione della firma, nella fornitura e revoca del consenso.

Gli Agenti sono adeguatamente istruiti dal Soggetto Erogatore ;

2.1.3 Soggetto Realizzatore

Unimatica 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 grazie alla piattaforma installata presso il proprio data-center.
Unimatica S.p.A. è leader di mercato per i processi di firma elettronica e conservazione sostitutiva dei documenti digitali a norma di legge e per i servizi di Posta Elettronica Certificata. Unimatica S.p.A. progetta e sviluppa soluzioni informatiche ad alto valore tecnologico per la dematerializzazione dei processi documentali di imprese, banche, compagnie di assicurazione, associazioni, ordini professionali, Pubblica Amministrazione e professionisti.
Con un capitale sociale di 500.000 euro, Unimatica S.p.A. eroga servizi di firma elettronica avanzata, qualificata e digitale, gestione documentale, conservazione a norma dei documenti, certificazione e sicurezza digitale, gestione di Posta Elettronica Certificata, dematerializzazione dei flussi documentali end-to-end.

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

Unimatica S.p.A. è inoltre la terza parte cui è affidata la custodia della chiave di decifratura dei dati biometrici, elemento essenziale nei processi di verifica della firma.

Denominazione Sociale	**Unimatica S.p.A.**
Sede legale	**Via Cristoforo Colombo, 21 – 40131 Bologna**
Partita IVA	**02098391200**
Numero iscrizione Registro delle Imprese	**REA BO 413696**
Sito Web	**www.unimaticaspa.it**

3 Regole Generali

3.1 Obblighi e Responsabilità

Nel presente capitolo, si descrivono le condizioni generali alle quali il Soggetto Erogatore AXA eroga il servizio di Firma Elettronica Avanzata.

3.1.1 Obblighi del Soggetto Realizzatore

Il Soggetto Realizzatore Unimatica S.p.A. è obbligato a garantire che:

a) La soluzione di firma grafometrica sviluppata sia conforme alle specifiche tecniche e funzionali definite con AXA;
b) La soluzione tecnologica sviluppata consenta la connessione univoca della firma al sottoscrittore;
c) La soluzione tecnologica sviluppata garantisca il controllo esclusivo del sottoscrittore del sistema di generazione della firma, ivi inclusi i dati biometrici di generazione della firma;
d) La soluzione tecnologica sviluppata utilizzi adeguate tecniche di cifratura dei dati biometrici raccolti e trattati, al fine di impedirne la visualizzazione "in chiaro";
e) il documento informatico non possa subire modifiche dopo l'apposizione della firma.

3.1.2 Obblighi del sottoscrittore

Il sottoscrittore è tenuto a:

a) Garantire la correttezza e la completezza dei dati personali forniti;
b) consegnare all'Agente o incaricato da parte di AXA di un documento di identità in corso di validità al momento della sottoscrizione del documento DAC;
c) prendere attenta visione della documentazione descrittiva del servizio FEA prima dell'adesione al servizio;
d) utilizzare il servizio FEA esclusivamente nei rapporti con AXA.

3.2 Assicurazione obbligatoria

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

4 Identificazione del sottoscrittore

Ai sensi dell'articolo 57 comma 1 lettera a) del **DPCM**, i soggetti erogatori della soluzione di FEA devono identificare in modo certo l'utente tramite un valido documento di riconoscimento.
Nel presente capitolo, si descrivono le modalità di identificazione, i soggetti abilitati e il processo di identificazione facente parte della soluzione di FEA Grafometrica AXA.

4.1 Identificazione ai fini dell'adesione

L'identificazione certa del sottoscrittore del documento è eseguita per conto di AXA da parte degli agenti esclusivamente in 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 (7)) sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente.

5 Operatività

5.1 Identificazione e adesione alla modalità di firma

Il processo di identificazione ed adesione alla modalità di firma, eseguito "una tantum" al primo utilizzo del servizio di firma elettronica e quando necessario registrare variazioni, si compone delle seguenti fasi:

1. l'Agente accede al sistema AXA attraverso il proprio web browser o la app installata sul tablet ed evidenzia la necessità di raccogliere e/o aggiornare il Modulo Anagrafico;
2. l'Agente raccoglie il documento di identità e ne verifica le informazioni, acquisendone una copia per immagine, mediante uno scanner o la fotocamera del device mobile;
3. le applicazioni informatiche AXA generano i PDF dell'acquisizione del documento d'identità e del Modulo Anagrafico e li consegna alla piattaforma di firma grafometrica Unimatica S.p.A.;
4. il cliente legge il Modulo Anagrafico su monitor o tablet e lo sottoscrive con la firma grafometrica, mediante il pad o direttamente sul tablet, utilizzando l'apposito pennino elettronico e conferma;
5. il pad o il tablet registrano i parametri biometrici primari associati alle firme della sottoscrizione.
6. la piattaforma di firma grafometrica raccoglie i dati biometrici e li cifra insieme all'impronta del contenuto sottoscritto (codice di hash), mediante una chiave pubblica, indi li inserisce all'interno del PDF del Modulo Anagrafico.
7. la piattaforma di firma grafometrica appone la firma digitale automatica appartenente a un soggetto AXA;
8. la piattaforma di firma grafometrica restituisce alle applicazioni informatiche di AXA il file in formato PDF contenente l'immagine del documento Modulo Anagrafico sottoscritto (PDF rendering);
9. le applicazioni informatiche AXA inviano all'indirizzo di posta elettronica dichiarato dal Cliente nel Modulo Anagrafico il file PDF rendering di quanto sottoscritto; a richiesta del cliente, l'Agente stampa una copia cartacea del Modulo Anagrafico;
10. la piattaforma di firma grafometrica invia il Modulo Anagrafico sottoscritto e la copia del documento di identità al sistema di Conservazione;
11. il sistema di conservazione, in carico a IDM (Integra Document Management S.r.l.), provvede alla conservazione per i 20 anni previsti dall'articolo 57 comma 1 lettera b) del DPCM del 22 febbraio 2013;

Tutte le variazioni ai dati e alle informazioni, nonché ai consensi forniti, devono essere effettuate compilando e sottoscrivendo un nuovo Modulo Anagrafico.

Dopo l'adesione al servizio, per la sottoscrizione di contratti e documenti, l'Agente si limiterà ad accertarsi della correttezza dell'identità del Cliente, senza acquisire nuovamente la copia del documento di identità, se in corso di validità.

5.2 Firma del documento

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

1. L'Agente accede al sistema AXA attraverso il proprio web browser o la app installata sul tablet ed elabora la proposta commerciale, che è salvata sugli applicativi AXA;

2. L'Agente seleziona la funzione che permette di firmare in modalità grafometrica il documento;
3. Gli applicativi informatici AXA generano il documento in formato PDF e lo inviano alla piattaforma di firma grafometrica.
4. Il Cliente prende visione del contratto in tutte le sue parti sfogliandolo mediante le apposite funzionalità e lo sottoscrive mediante il pad o direttamente sul tablet, utilizzando l'apposito pennino elettronico e conferma;
5. Il pad o il tablet registrano i parametri biometrici primari associati alla firma.
6. I dati biometrici raccolti, insieme all'impronta del contenuto sottoscritto (codice di hash), sono crittografati dalla piattaforma di firma grafometrica utilizzando una chiave pubblica, indi inseriti nel documento . Il procedimento consente di garantire l'immodificabilità del documento nel tempo e l'impossibilità di estrarre i dati biometrici stessi dal PDF per riutilizzarli su un altro documento;
7. La piattaforma di firma grafometrica procede quindi all'apposizione di una o più firme digitali appartenenti a soggetti AXA, secondo la tipologia di documenti, con procedura automatica, a garanzia della sua autenticità;
8. La piattaforma di firma grafometrica restituisce alle applicazioni AXA un file in formato PDF contenente l'immagine del documento sottoscritto e della sottoscrizione apposta (PDF rendering);
9. Le applicazioni AXA inviano all'indirizzo elettronico dichiarato dal Cliente nel Modulo Anagrafico il PDF rendering di quanto sottoscritto. Su richiesta del cliente, l'Agente stampa una copia cartacea del Modulo Anagrafico;
10. La piattaforma di firma grafometrica invia il documento completo al sistema di conservazione.
11. Il sistema di conservazione prende in carico il documento completo e lo inserisce nell'archivio sostitutivo specifico. Il documento verrà conservato nel sistema di conservazione a norma per il periodo normativo previsto.

5.3 Soluzione tecnologica utilizzata

La soluzione tecnologica utilizzata si compone di quattro macro-elementi: la postazione dell'Agente con il pad di raccolta di firma, che può essere anche un tablet, le applicazioni AXA di creazione del documento, la piattaforma di firma grafometrica Unimatica S.p.A., integrata con i servizi di certificazione digitale e il sistema di conservazione del documento informatico affidato a IDM (Integra Document Management S.r.l.).

5.3.1 Postazione dell'Agente

La postazione dell'Agente coincide con il proprio PC (anche Tablet) utilizzato per l'operatività, allestito per poter raccogliere la firma grafometrica.

La soluzione tecnologica prescelta utilizza dispositivi hardware dotati di tecnologia *touch* in grado di rilevare i principali parametri della firma dell'utente dispositivi utilizzati possono afferire a due categorie:

- pad di firma: dispositivi di raccolta collegati a mezzo cavo USB, il documento è visualizzato al Cliente su un secondo monitor ovvero, se le dimensioni del pad lo consentono, direttamente sul dispositivo;
- dispositivi mobili: tablet dotati di connettività che consentono di visualizzare direttamente il documento e raccogliere la firma del cliente e i parametri biometrici connessi.

5.3.2 Applicazioni informatiche AXA

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

5.3.3 Piattaforma di firma grafometrica

La postazione dell'Agente e le applicazioni informatiche AXA colloquiano con la piattaforma di firma grafometrica installata presso il data-center Unimatica S.p.A. che svolge le seguenti operazioni:

- Raccolta dati biometrici rilevati dal dispositivo;
- Cifratura dei dati biometrici;
- Inserimento sicuro dei dati nel contratto;
- Apposizione, mediante procedura automatica, di firma digitale appartenente a soggetti AXA, a chiusura del processo di firma grafometrica, a presidio dell'integrità del documento e dei dati biometrici crittografati;
- Creazione del file in formato PDF dell'immagine del documento firmato per la restituzione alle applicazioni AXA;
- Versamento della documentazione al sistema di Conservazione per garantire disponibilità, integrità, leggibilità e autenticità nel tempo;

5.3.4 Sistema di conservazione

IDM (Integra Document Management S.r.l.) svolge il ruolo di Responsabile della Conservazione dei documenti in base all'atto di affidamento a questo scopo sottoscritto da AXA, per la delega dei compiti e delle responsabilità ad IDM (Integra Document Management S.r.l.). come soggetto terzo dotato di adeguata competenza ed esperienza, ai sensi della deliberazione CNIPA 11/04, articolo 5, comma 2.

La piattaforma di firma grafometrica installata presso il data-center Unimatica S.p.A. invia i PDF relativi al documento firmato al sistema di conservazione di IDM che si occupa delle seguenti attività.

- Verifica integrità flussi dati ricevuti;
- Inserimento documenti nel sistema di conservazione sostitutiva a norma e registrazione dei dati di catalogazione del documento;
- Creazione lotti di conservazione (creazione di un lotto di conservazione con tutti i documenti ricevuti nella giornata)
- Apposizione firma digitale del responsabile della conservazione al lotto di conservazione.
- Apposizione marca temporale rilasciata da una Certification Autority al lotto di conservazione.
- Memorizzazione dei lotti di conservazione su dispositivi di storage ad alta affidabilità e generazione copia di sicurezza su unità di DR/backup Conservazione a norma dei documenti pe il periodo normativo prestabilito;
- Conservazione digitale dei documenti secondo le modalità definite dalla normativa vigente (DPCM 3 dicembre 2013).

6 Controllo del sistema di sottoscrizione

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

6.1 Strumenti per il controllo del sistema

Presso il data-center Unimatica S.p.A. sono attivi strumenti di controllo automatico che consentono di valutare gli eventi e gli stati in cui il sistema viene a trovarsi.
Il sistema e configurato in modo da intraprendere, in funzione dell'evoluzione dei suoi stati, delle azioni fra le seguenti tipologie:

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

6.2 Verifiche di sicurezza e qualità

Le procedure operative e le procedure di sicurezza di Unimatica S.p.A. sono soggette a controlli periodici legati sia alla verifiche ispettive per il conseguimento ed il successivo mantenimento delle certificazioni dei Sistemi di Gestione (Sistema di Gestione della Qualità ISO 9001, Sistema di Gestione della Sicurezza delle Informazioni ISO 27001) 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.

7 Misure di sicurezza

Il sistema di firma elettronica avanzata in modalità grafometrica è protetto da numerose misure di sicurezza poste a presidio dei dati del Cliente e dei documenti sottoscritti. Le misure di sicurezza sviluppate da AXA per la protezione delle postazioni di lavoro degli Agenti, sia fisse che in mobilità, sono completate dalle misure di sicurezza Unimatica S.p.A., poste a protezione del data-center da cui sono erogati i servizi di firma elettronica.

7.1 Misure di sicurezza Unimatica S.p.A.

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

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

7.1.1 Sicurezza fisica

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

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

7.1.2 Sicurezza delle procedure

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

7.1.3 Sicurezza logica

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

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

Unimatica S.p.A. 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.

8 Cessazione del servizio

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

8.1 Revoca del consenso da parte del cliente

In caso il Cliente scelga di revocare il proprio consenso all'utilizzo del servizio di FEA, secondo la procedura descritta al paragrafo seguente, dal momento della revoca i documenti che regolano i rapporti tra il Cliente e 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.

8.2 Procedura per la revoca del consenso

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

8.3 Dismissione del servizio FEA

Qualora AXA 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, che continueranno ad essere conservati a norma da AXA per tutto il termine di conservazione previsto.
AXA continuerà a conservare inoltre il Modulo Anagrafico 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.

9 Contatti

9.1 Contatto per assistenza

Qualora necessario, i Clienti che necessitino di assistenza, informazioni aggiuntive sul servizio di firma elettronica e cessazione del servizio possono rivolgersi al proprio Intermediario od all'Assistenza fornita da AXA mediante contact center.

9.2 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 contenente l'immagine de

- il Documento Anagrafico Consensi (DAC) 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.

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

In caso di necessità dei documenti originale, esclusivamente a comprovati fini di produzione in giudizio o esibizione di fronte alla Pubblica Autorità, il Cliente può chiedere l'apertura e verifica del documento presso il Notaio.
I documenti sono forniti all'indirizzo e-mail dichiarato e sono duplicati informatici contenenti i dati biometrici e corredati dalle evidenze informatiche di corretta conservazione6 prodotti da IDM (Integra Document Management S.r.l.).

6 File in formato P7m che conterrà il documento in formato PDF e i dati della firma digitale del responsabile della conservazione nonché il riferimento temporale della data di avvenuta conservazione.