Firma Elettronica Avanzata in modalità Grafometrica

Manuale Operativo 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 rivolto ad un utilizzo combinato con il documento "Modulo di adesione al servizio di firma elettronica avanzata in modalità grafometrica erogato da Sara Assicurazioni S.p.A." (di seguito anche Modulo di Adesione) e rappresenta il documento riassuntivo delle caratteristiche tecniche del servizio di firma elettronica.

1.2 Riferimenti normativi e tecnici

Riferimenti normativi

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

1.3 Definizioni

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

Certificato Qualificato	• il certificato elettronico conforme ai requisiti di cui all'allegato I della Direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva (art 1, comma 1 lettera f CAD)
Certificato, Certificato Digitale	• Insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica. • Nel certificato compaiono altre informazioni tra cui: o il Certificatore che lo ha emesso o il periodo di tempo in cui il certificato può essere utilizzato; o altri campi (estensioni) che determinano caratteristiche aggiuntive al certificato.
Certificatore [Certification Authority]	• il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime (art 1, comma 1 lettera g **CAD**)
Chiave privata	• l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico. (art 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 firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare il controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art 1, comma 1 lettera q-bis **CAD**)
Firma elettronica qualificata	• Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art 1, comma 1 lettera r **CAD**)
Firma Grafometrica	• un particolare tipo di firma elettronica ottenuta grazie al rilevamento dinamico dei dati calligrafici (ritmo, pressione, velocità, inclinazione della penna, movimento, ecc.) della firma di un individuo tramite una penna elettronica su specifici dispositivi idonei a rilevare le caratteristiche sopra indicate
[Hash] / impronta	• la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione a una evidenza informatica di una opportuna funzione di hash (articolo 1, co. 1, lettera h **DPCM**)
Funzione di hash	• una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguale a partire da evidenze informatiche differenti (articolo 1, co. 1, lettera g **DPCM**)
Marca temporale [Time Stamp Token]	• il riferimento temporale che consente la validazione temporale (articolo 1, co. 1, lettera i **DPCM**)
Modulo di Adesione	• documento contrattuale elaborato da Sara che raccoglie i consensi del cliente in merito all'utilizzo del sistema di firma elettronica, stipulato dal cliente una tantum all'inizio del rapporto o in un momento successivo
Responsabile della Conservazione	• soggetto responsabile del sistema di conservazione dei documenti
Pad	• tavoletta che consente di visualizzare direttamente il documento e raccogliere la firma del cliente e i parametri biometrici connessi
XML	• Extensible Markup Language, metalinguaggio utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati.

2 Generalità

La fattispecie “firma elettronica avanzata” è stata introdotta nel nostro ordinamento dal decreto legislativo 30 dicembre 2010, n. 235 di modifica del codice dell’amministrazione digitale (il D.Lgs. n. 82/2005, **CAD**), che ha inserito una nuova definizione alla lettera q-bis) dell’art. 1: “insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l’identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati”.

Dal punto di vista probatorio, il medesimo decreto legislativo n. 235/2010 ha inoltre stabilito che:

> “2. 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. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.
>
> 2-bis). Salvo quanto previsto dall’articolo 25, le scritture private di cui all’articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale”.

C’è quindi una norma chiara che consente di sottoscrivere con la Firma Elettronica Avanzata i documenti per cui è necessaria una forma scritta, sia essa *ad sustantiam* o *ad probationem*, come le polizze assicurative o i contratti di finanziamento.

Dalle previsioni del **CAD**, tuttavia, non emerge in maniera chiara la natura della nuova figura di “firma elettronica avanzata”. Secondo la definizione se ne può desumere unicamente che: 1) si tratta di un insieme di dati in forma elettronica; 2) connessi ad un documento informatico; 3) che identificano il firmatario del documento; 4) garantiscono la “connessione univoca con il firmatario”; 5) creati con mezzi sui quali il firmatario può conservare un controllo esclusivo; 6) e che consentono di rilevare se i dati stessi sono stati successivamente modificati.

Per poter sostanziare nella pratica una FEA, è infatti necessario il rispetto delle regole tecniche, altrimenti lo strumento si sostanzia come firma elettronica semplice.

Per l’emanazione delle regole tecniche, AgID (Agenzia per l’Italia Digitale) ha istituito dei gruppi di lavoro per la definizione delle regole tecniche e linee guida relative a una serie di argomenti (Formazione del documento informatico, sistema di conservazione, gestione dei flussi documentali, identità digitali, continuità operativa e infrastrutture critiche nella P.A., ecc), tra cui anche il gruppo di lavoro per la definizione delle regole tecniche di firma digitale, validazione temporale e firma elettronica avanzata.

Le regole tecniche, contenute nel DPCM 22 febbraio 2013 pubblicato nella Gazzetta Ufficiale n. 117 del 21 maggio 2013, non contengono alcun accenno alle tecnologie di firma da utilizzare. L’art. 56, rubricato “Caratteristiche delle soluzioni di firma elettronica avanzata” non offre alcuna informazione aggiuntiva al riguardo, limitandosi a “scomporre” ed esplicitare i requisiti già contenuti nella definizione di cui all’art. 1, lett. q bis) del C.A.D.

La vera novità riguarda invece l'ambito di operatività delle firme elettroniche avanzate. L'art. 55 delle regole tecniche, comma 2°, infatti, chiarisce che possono essere sviluppate soluzioni con tale tecnologia di firma: a) o internamente, al fine di utilizzarle nel processo di dematerializzazione dei rapporti intrattenuti con terzi; b) oppure al fine di commercializzarle sul mercato.

L'art. 60, a sua volta, stabilisce che la firma elettronica avanzata è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto che intende utilizzarla al fine della dematerializzazione dei documenti.

In questo contesto si inserisce la fattispecie di firma grafometrica, ossia un particolare tipo di firma elettronica che si ottiene dal rilevamento dinamico dei dati calligrafici (ritmo, pressione, velocità, inclinazione della penna, movimento, ecc.) della firma di un individuo tramite una penna elettronica.

La firma grafometrica viene apposta tramite l'utilizzo di specifici "SignaturePad", idonei a rilevare le caratteristiche sopra indicate dei dati calligrafici che costituiscono i "dati biometrici" del sottoscrittore. La soluzione di firma grafometrica, a fronte di un valido riconoscimento del sottoscrittore, deve consentire di assicurare il rispetto dei requisiti per la validità della firma elettronica avanzata.

La soluzione di Firma Elettronica Avanzata, sia essa in modalità grafometrica o in altre modalità, è quindi una soluzione che si avvale della tecnologia, che deve tuttavia essere integrata da una serie di procedure operative e di informative date al titolare della firma.

Questo documento evidenzia le regole generali e le procedure seguite dal Soggetto Erogatore Sara Assicurazioni S.p.A. (nel proseguo indicato semplicemente come: "Sara") per l'erogazione e l'utilizzo del servizio di Firma Elettronica Avanzata in modalità grafometrica (nel proseguo semplicemente indicata come FEA o Firma Grafometrica).

2.1 Attori

2.1.1 Soggetto Erogatore

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

Come previsto dall'articolo 60 del DPCM, la soluzione di firma grafometrica è utilizzata esclusivamente nell'ambito dei rapporti giuridici intercorrenti tra Sara e il sottoscrittore, restando escluso ogni altra possibilità di utilizzo.

Denominazione Sociale:	**Sara assicurazioni spa**
Sede Legale :	Via Po 20 Roma
Sedi Operative	
Partita IVA	00885091009
Numero iscrizione Registro delle Imprese	
Sito Web	http://www.sara.it/
PEC:	saraassicurazioni@sara.telecompost.it

2.1.2 Agenzie

Nello svolgimento delle proprie attività di Soggetto Erogatore, Sara si avvale dei propri agenti, i quali svolgono le attività di:

- Identificare il firmatario;
- Raccogliere la copia del documento di identità;
- Raccogliere la sottoscrizione del cliente della dichiarazione di adesione al servizio di FEA (Modulo di Adesione), per accettazione delle condizioni del servizio da parte dell'utente stesso.
- Supporto operativo al firmatario nell'apposizione della firma, nella fornitura e nella revoca del consenso.

Sara informa le Agenzie mediante specifiche circolari interne che dettagliano il processo da seguire.

2.1.3 Soggetto Realizzatore

Il servizio viene realizzato mediante l'adozione di una soluzione tecnologica che comporta la cooperazione dei seguenti soggetti:

- InfoCert S.p.A., che i) cura l'implementazione, la gestione applicativa e la manutenzione della soluzione di firma grafometrica presso Sara, ii) svolge l'attività di conservazione dei dati biometrici e dei documenti informatici sottoscritti con firma grafometrica, iii) fornisce in qualità di Certification Autorithy il certificato di firma automatica di Sara con cui "chiude" i documenti;

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

- Euronovate SA, che fornisce i) il software di raccolta della sottoscrizione in modalità grafometrica impiegato nella soluzione di firma grafometrica stessa;

Denominazione Sociale	**Euronovate SA**
Sede Legale	Via Pian Scairolo, 11 6915, Lugano (Svizzera)
Partita IVA	CHE-224.841.103
Sito Web	http://www.euronovate.com/
Mail	info@euronovate.com

La soluzione di FEA realizzata da InfoCert S.p.A. utilizza i servizi di certificazione digitale di InfoCert medesima, Certification Authority di riferimento per l'acquisizione degli strumenti certificati di firma digitale che intervengono nel processo ed il software di raccolta della sottoscrizione grafometrica di Euronovate SA, opportunamente integrato da proprie applicazioni all'interno della soluzione fornita a Sara.

InfoCert svolge inoltre il ruolo di responsabile dei servizi di conservazione dei documenti in base all'atto di affidamento a questo scopo sottoscritto da Sara, per la delega dei compiti e delle responsabilità ad InfoCert come soggetto terzo dotato di adeguata competenza ed esperienza, ai sensi del DPCM 3 dicembre 2013.

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

3 Regole Generali

3.1 Obblighi e Responsabilità

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

3.1.1 Obblighi del Soggetto Erogatore

Il Soggetto Erogatore è tenuto a garantire che:

a) siano rispettate le regole tecniche di cui al DPCM;

b) il firmatario sia preventivamente identificato tramite un valido documento di riconoscimento;

c) il firmatario sia preventivamente informarto in merito agli esatti termini e condizioni relative all'uso del servizio, compresa la limitazione dell'uso;

d) l'attivazione del servizio di FEA sia subordinata alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte del Firmatario;

e) copia del documento di riconoscimento e la dichiarazione di cui alla lettera precedente siano conservate per almeno 20 anni, garantendone la disponibilità, integrità, leggibilità e autenticità;

f) il firmatario possa ottenere su richiesta e gratuitamente copia della dichiarazione e tutte le informazioni sulla soluzione al firmatario;

g) siano presenti tutte le informazioni definite dal DPCM sul proprio sito internet, compreso il presente documento;

h) sia possibile per il Firmatario la revoca del consenso all'utilizzo della soluzione di firma elettronica avanzata;

i) sia fornito al Firmatario un servizio di assistenza;

j) la Firma Elettronica Avanzata sia apponibile solamente da parte del Firmatario;

k) il Firmatario abbia la piena coscienza del documento che sta sottoscrivendo, e non sia possibile che la propria sottoscrizione possa essere apposta su un documento differente da quello visualizzato;

l) non sia possibile riutilizzare la sottoscrizione apposta dal Firmatario su un differente documento informatico.

3.1.2 Obblighi del Soggetto Realizzatore

Il Soggetto Realizzatore è tenuto a garantire che:

a) la soluzione di firma grafometrica sviluppata sia conforme alle specifiche tecniche e funzionali definite con Sara;

b) la soluzione tecnologica sviluppata consenta la connessione univoca della firma al firmatario;

c) la soluzione tecnologica sviluppata garantisca il controllo esclusivo del firmatario 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.

3.1.3 Obblighi del Firmatario

Il Firmatario è tenuto a garantire:

a) la correttezza e la completezza dei dati personali forniti;

b) la consegna all'addetto di sportello di un documento di identità in corso di validità al momento della sottoscrizione del Modulo di Adesione;

c) di aver preso visione della documentazione descrittiva del servizio FEA prima dell'adesione al servizio.

3.2 Assicurazione obbligatoria

Ai sensi dell'articolo 57 comma 2 Sara ha stipulato una idonea copertura assicurativa per la responsabilità civile, al fine di proteggere i titolari della firma elettronica avanzata e i terzi da eventuali danni cagionati da inadeguate soluzioni tecniche. I massimali sono quelli previsti dal DPCM, ovvero un ammontare non inferiore a euro 500.000.

4 Processo di identificazione e sottoscrizione

Ai sensi dell'articolo 57 comma 1 lettera a) del DPCM, i soggetti erogatori della soluzione di FEA devono identificare in modo certo l'utente tramite un valido documento di riconoscimento al fine di configurare una firma elettronica avanzata correttamente formata.

Ai sensi dell'articolo 60 del DPCM e come dettagliato dal Modulo di Adesione, la firma elettronica avanzata in modalità grafometrica è utilizzabile esclusivamente nei rapporti intercorrenti tra il firmatario e Sara.

In questo capitolo si descrivono le modalità operative previste per l'identificazione dell'utente, l'adesione al servizio di FEA grafometrica e la sottoscrizione dei documenti in modalità di FEA grafometrica, facenti parte della soluzione di FEA Grafometrica erogata da Sara.

4.1 Identificazione del firmatario

L'identificazione certa del firmatario del documento è eseguita da Sara avvalendosi della propria rete di agenti (o personale incaricato dall'agente) sparsi su tutto il territorio nazionale. L'identificazione è svolta sempre in presenza del firmatario e ad ogni apposizione di firma grafometrica viene accertata l'identità dello stesso dall'operatore d'agenzia l'agente o personale da lui incaricato verifica l'identità del firmatario tramite il riscontro con uno dei seguenti documenti, valido e non scaduto, secondo quanto previsto dall'art. 35, Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445:

- Carta d'identità
- Passaporto
- Patente di guida
- Patente nautica
- Libretto di pensione
- Patentino di abilitazione alla conduzione di impianti termici
- Porto d'armi

Sono ammesse ulteriori tessere di riconoscimento oltre a quelle indicate, purché munite di fotografia e di timbro, rilasciate da un'amministrazione dello Stato.

4.2 Inserimento dei dati anagrafici

L'agente o personale da lui incaricato, ricevuto il cliente, inserisce tutti i dati necessari all'operazione in corso sull'applicativo Sara che governa l'emissione dei documenti contrattuali. L'applicativo Sara verifica se il cliente ha già aderito al servizio di Firma Elettronica Avanzata e, in caso negativo, l'agente o personale da lui incaricato domanda al cliente presente in agenzia se è intenzionato ad aderire al servizio di firma elettronica avanzata attraverso la modalità grafometrica. In caso di rifiuto del cliente il processo di raccolta dell'adesione al servizio di firma grafometrica si interrompe e si procede con il sistema cartaceo al di fuori dal campo di applicazione del presente documento.

4.3 Acquisizione documento

Il cliente che abbia espresso la propria intenzione di sottoscrivere con la modalità grafometrica viene identificato in modo certo dall'operatore mediante la richiesta di un documento d'identità in corso di validità in conformità alla normativa di riferimento (citata al punto 4.1 del presente documento). Nella sola fase di adesione al servizio di firma grafometrica, detto documento di identità verrà acquisito otticamente ed allegato al modulo di adesione di cui al punto 4.4.

4.4 Firma modulo d'adesione

Una volta identificato il firmatario e raccolto il documento di identità, al cliente viene sottoposto sul SignaturePad il modulo di adesione, comprendente sia la dichiarazione di adesione ai servizi di firma elettronica avanzata, sia il consenso al trattamento dei dati personali, affinché il cliente possa leggerlo. In caso di richiesta da parte del cliente l'agente o personale da lui incaricato potrà stampare il modulo, presente sul sito web, per consentirne la visione al cliente.

Il modulo di adesione così firmato e l'allegato documento di identità sono conservati a norma per almeno 20 anni. L'adesione vale fino a successiva eventuale revoca del cliente e pertanto non sarà necessaria ulteriore adesione in fase di firma dei successivi singoli documenti contrattuali.

Dopo l'apposizione delle firme del modulo sul SignaturePad, il modulo così sottoscritto viene inviato via mail all'indirizzo eventualmente fornito dal cliente. Qualora il cliente non fornisca alcun indirizzo mail, l'agente provvederà alla stampa del modulo di adesione ed alla consegna al cliente.

4.5 Firma della documentazione Sara.

Una volta raccolta l'adesione, il cliente potrà firmare in modalità grafometrica tutti i documenti contrattuali e precontrattuali stipulati con Sara per i quali la Compagnia avrà reso, nel corso del tempo, disponibile tale servizio. L'utilizzo della firma grafometrica sarà possibile in modo graduale, aumentando progressivamente nel tempo le tipologie di documenti sottoscrivibili dal cliente con questa nuova modalità di firma. Il cliente potrà comunque sempre chiedere che si proceda alla sottoscrizione con il sistema cartaceo al di fuori dal campo di applicazione del presente documento.

L'agente o personale da lui incaricato selezionerà l'apposita funzionalità che consente di firmare i documenti in modalità grafometrica. Gli applicativi Sara generano il documento in formato PDF e lo inviano alla piattaforma di firma grafometrica. I documenti possono pertanto essere visualizzati sul SignaturePad affinchè il cliente possa leggerli. Il cliente potrà infine procedere alle firme sul SignaturePad.

Firmati i documenti sul SignaturePad, gli stessi vengono inviati via mail all'indirizzo eventualmente fornito dal cliente. Qualora il cliente non fornisca alcun indirizzo mail, l'agente provvederà alla stampa della documentazione ed alla consegna al cliente.

4.6 Verifiche conclusive

Viene effettuata una verifica da parte del sistema di InfoCert sul pacchetto documentale e sulla correttezza e validità di tutta la documentazione raccolta in base agli attributi inviati dai sistemi Sara in sede di apertura pratica. L'applicativo sviluppato da InfoCert (LegalBus) verifica l'effettiva esecuzione di tutti task necessari e le operazioni obbligatorie. La chiusura della pratica con il relativo invio in conservazione verrà effettuato solo al termine della effettiva elaborazione (acquisizione, firma, visualizzazione, invio). In assenza di tutti gli attributi necessari il pacchetto rimane in sospeso. La documentazione correttamente formata, verrà inviata ai sistemi di conservazione sostitutiva di InfoCert in quanto incaricata del servizio di conservazione.

5 Soluzione tecnologica utilizzata

La soluzione tecnologica utilizzata si compone di due macro-elementi: la postazione di sportello con il SignaturePad di visualizzazione del documento e raccolta di firma e le componenti software che costituiscono la piattaforma di firma grafometrica, fra cui, come indicato, il software Euronovate SA ed i moduli InfoCert, integrata questi ultimi a loro volta integrati con i servizi di certificazione digitale e conservazione del documento informatico di InfoCert medesima.

5.1 Postazione di sportello

La postazione di sportello coincide con il PC utilizzato per l'operatività classica di sportello, allestito con uno specifico SignaturePad 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. Il dispositivo utilizzato è un SignaturePad collegato a mezzo cavo USB al PC di sportello, su quale viene anche visualizzato il documento o un estratto di esso al Cliente.

5.2 Componenti software

Le componenti software, consentono agli agenti di Sara lo svolgimento dell'operatività di sportello, sottoponendo alla firma grafometrica i documenti informatici. La piattaforma di firma grafometrica installata presso il data-center InfoCert svolge le seguenti operazioni:

- ricezione dell'intero pacchetto relativo alla pratica da trattare;
- presentazione all'utente di una check List in base alla tipologia documentale richiesta;
- raccolta del documento d'identità ove richiesto;
- raccolta dati biometrici rilevati dal dispositivo;
- cifratura dei dati biometrici;
- inserimento sicuro dei dati nel documento;
- firma digitale del documento a chiusura del processo di firma grafometrica;
- stampa delle copie da consegnare all'utente.

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

La stessa piattaforma provvede alla restituzione di copia dei documenti sottoscritti al sistema di gestione documentale utilizzato da Sara, ed all'invio del documento al sistema di conservazione InfoCert.

5.2.1 Servizio di firma digitale automatica

A chiusura del processo di firma grafometrica del documento, grazie al servizio di firma digitale automatica InfoCert, Sara appone la firma digitale di uno o più suoi addetti attraverso una procedura automatica, a presidio dell'integrità del documento e dei dati biometrici crittografati.

Le chiavi dei soggetti titolari dei certificati di firma digitale sono generate e conservate presso InfoCert, su dispositivi sicuri ad alte prestazioni (Hardware Security Module o HSM).

5.2.2 Servizio di conservazione elettronica a norma

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

Il servizio garantisce il pieno rispetto della normativa vigente in materia di conservazione elettronica dei documenti; Sara ha delegato ad InfoCert le responsabilità previste dalla normativa vigente sul procedimento di conservazione elettronica dei documenti.

InfoCert, in qualità di responsabile del processo di conservazione, garantisce il soddisfacimento di tutti i requisiti necessari per preservare la validità legale nel tempo dei documenti conservati. Le componenti software della soluzione di firma grafometrica inviano in conservazione i documenti corredati da opportuni indici di ricerca, in modo da rendere più efficaci ed agevoli le attività di ricerca della documentazione conservata, che avviene da parte degli addetti Sara in modalità sicura e profilata.

Il servizio offre inoltre agli addetti Sara apposite funzioni di esibizione che consentono di consultare, oltre al contenuto del documento, le attestazioni relative al buon esito del processo di conservazione, che costituiscono una esibizione valida e non opponibile in caso di verifiche, controlli ed ispezioni da parte della Pubblica Autorità.

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

Il Data Center InfoCert è gestito seguendo le best practice suggerite dall'ITIL (Information Technology Infrastructure Library).Le strumentazioni di controllo sono state implementate su progetti open source come il Nagios, tramite il quale si realizza il monitoraggio completo dei servizi di business offerti da InfoCert.

Le console operative del data center sono controllate dagli operatori durante l'orario di presidio. Sulle console operative vengono riportati, per ogni singolo server oggetto di controllo, tutte le informazioni raccolte dagli agenti e che richiedono l'attenzione degli operatori. Al di fuori di tali orari è previsto un servizio di reperibilità degli operatori del Service Desk che vengono avvisati in caso di anomalie dai sistemi di controllo automatici, tramite un sistema di notifica automatica SMS.

Il personale non si collega direttamente al singolo server, ma opera attraverso l'utilizzo di un sistema, sviluppato dalla funzione aziendale che sovraintende alla sicurezza informatica, che prevede la verifica delle credenziali di accesso personali anche attraverso l'utilizzo di certificati di autenticazione. Gestisce inoltre la profilazione e le autorizzazioni di ciascun utente e provvede a loggare le attività svolte sui vari sistemi da ogni singolo operatore.

6.2 Verifiche di sicurezza e qualità

Le procedure operative e le procedure di sicurezza di InfoCert sono soggette a controlli periodici legati sia alla verifiche ispettive per il conseguimento ed il successivo mantenimento delle certificazioni del Sistema di Gestione della Qualità ISO 9001/27001 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 Sara per la protezione delle postazioni di sportello sono completate dalle misure di sicurezza InfoCert poste a protezione dei servizi erogati.

7.1 Misure di sicurezza Sara

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 Sara per la protezione delle postazioni di sportello sono completate dalle misure di sicurezza InfoCert poste a protezione dei servizi erogati. Entrambe le società ospitano le applicazioni che erogano i servizi di firma elettronica in datacenter ridondati per l'alta affidabilità e la business continuity, minimizzando i rischi derivanti dal malfunzionamento dei sistemi, della rete e delle applicazioni, oltre che dall'intercettazione non autorizzata o dalla modifica dei dati.

7.2 Misure di sicurezza Infocert

InfoCert ha realizzato il sistema all'interno del proprio data-center, dal quale vengono erogati anche 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.

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 Sara. 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 Sara saranno sottoscritti mediante firma autografa su carta.

Restano salvi i documenti precedentemente sottoscritti con firma elettronica avanzata in modalità grafometrica.

8.1.1 Procedura per la revoca del consenso

Il cliente può revocare la dichiarazione di adesione al servizio di Firma grafometrica direttamente nell'Agenzia presso la quale ha fornito l'Adesione al servizio. L'agenzia, identificato il cliente, provvederà a registrare l'avvenuta revoca direttamente sui sistemi di Sara, La revoca risulta, dunque, tracciata informaticamente (ai fini dell'esatta individuazione della data di presa in carico ed evasione della richiesta formulata).

A seguito della registrazione della revoca, viene inviata una comunicazione via SMS e/o via email al cliente - che abbia fornito il cellulare e/o l'indirizzo email - con cui si dà evidenza dell'operazione eseguita.

A seguito della revoca, non sarà più possibile per il cliente firmare con la modalità grafometrica salvo successiva nuova adesione. In alternativa il cliente potrà manifestare la propria volontà di revoca inviando apposita comunicazione a mezzo raccomandata all'indirizzo Sara assicurazioni SPA via Po 20 00198 Roma ovvero, ancora, via PEC all'indirizzo saraassicurazioni@sara.telecompost.it.

8.2 Dismissione del servizio FEA

Qualora Sara decidesse di dismettere il servizio di FEA, i documenti che regolano i rapporti tra il Cliente e Sara 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 InfoCert per tutto il termine di conservazione previsto.

Sara continuerà a conservare inoltre il Modulo di Adesione 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

Il cliente che necessiti di assistenza o informazioni aggiuntive sul servizio, può rivolgersi presso l'agenzia cui ha fornito l'adesione al servizio stesso ovvero presso la quale ha apposto firme su documenti contrattuali in modalità grafometrica.

Il presente documento relativo alle condizioni di utilizzo del servizio di firma grafometrica e delle tecnologie utilizzate è pubblicato sul sito internet www.sara.it.

9.2 Procedura di richiesta dei documenti

Il Cliente può ottenere in qualunque momento copia di tutta la documentazione relativa al servizio di firma elettronica avanzata o con questa sottoscritta.

In particolare è possibile ottenere copia o duplicato:

- del Modello di Adesione sottoscritto all'adesione al servizio
- del documento di identità allegato al modello di adesione
- dei documenti sottoscritti con la firma grafometrica

I documenti vanno richiesti direttamente all'agenzia presso la quale sono stati sottoscritti con la modalità di firma grafometrica, che provvederà a fornirli al cliente inviandoli via mail all'indirizzo eventualmente fornito dal cliente . I documenti sono forniti sotto forma di copia per immagine non contenente i dati biometrici per ragioni di sicurezza. E' prevista la possibilità che l'agente stampi la copia del documento richiesto in formato cartaceo, su richiesta da parte del cliente.

In caso di necessità dei documenti originali, esclusivamente su richiesta delle Autorità di polizia e/o dell'Autorità giudiziaria e ai fini di produzione in giudizio, il Cliente può chiedere a Sara l'esibizione della documentazione **in originale**. I documenti sono forniti al richiedente seguendo procedure di sicurezza rigorose nella piena osservanza delle disposizioni del Garante della Privacy; trattasi di duplicati informatici contenenti i dati biometrici e corredati dalle evidenze informatiche di corretta conservazione[1] prodotti da InfoCert.

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

10 Appendice A: Quadro sinottico del rispetto dei requisiti FEA

Si presenta di seguito il quadro sinottico dei requisiti previsti dal **DPCM** per la costruzione del sistema di firma elettronica avanzata, dettagliando i paragrafi del presente documento che illustrano le modalità di rispetto degli stessi.

Alcuni requisiti sono particolarmente cruciali e quindi sono evidenziati nel quadro sinottico con un asterisco (*****). L'articolo 56 comma 2 del **DPCM** prevede infatti che la firma elettronica avanzata generata in violazione di uno o più di questi requisiti "non soddisfa i requisiti previsti dagli articoli 20, comma 1-bis, e 21, comma 2, del Codice", ovvero il documento informatico così formato non ha l'efficacia prevista dall'articolo 2702 del codice civile (scrittura privata), né si applica la disposizione che prevede che "l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità".

#	rif. Normativo	Requisiti		Modalità di rispetto del requisito
1	**DPCM** art 56.1.a) **DPCM** art 57.1.a)	identificazione del firmatario del documento	*	• procedure di identificazione [§ 4]
2	**DPCM** art 56.1.b)	connessione univoca della firma al firmatario	*	• identificazione certa del cliente [§ 4.1] • firma in presenza dell'incaricato [§ 4.2] • acquisizione dei dati di biometria comportamentale [§5.1]
3	**DPCM** art 56.1.c)	controllo esclusivo del firmatario del sistema di generazione della firma	*	• dati di biometria comportamentale [§5.2]
4	**DPCM** art 56.1.d)	possibilità di verificare che l'oggetto di sottoscrizione non abbia subito modifiche dopo l'apposizione della firma	*	• procedura di inserimento dei dati biometrici nel PDF e l'apposizione della firma digitale a chiusura del processo [§ 5.2]
5	**DPCM** art 56.1.e)	possibilità per il firmatario di ottenere evidenza di quanto sottoscritto	*	• deposito del documento firmato sul portale • eventuale invio al firmatario del documento PDF rendering tramite posta elettronica o stampa cartacea su richiesta [§4.5 e 9.2]
6	**DPCM** art 56.1.f)	individuazione del soggetto erogatore della soluzione		• Modulo di Adesione • Manuale Operativo del Servizio
7	**DPCM** art 56.1.g)	assenza di qualunque elemento nel documento atto a modificarne gli atti, i fatti o i dati nello stesso rappresentati	*	• utilizzo del formato PDF • firma digitale a chiusura del processo [§5.2]
8	**DPCM** art 56.1.h)	connessione univoca della firma al documento sottoscritto	*	• procedura di inserimento dei dati biometrici nel PDF, con calcolo dell'hash del documento e apposizione della firma digitale a chiusura del processo [§5.2]
9	**DPCM** art 57.1.a)	identificazione certa dell'utente tramite un valido documento di riconoscimento		• identificazione certa del cliente [§ 4.1]
10	**DPCM** art 57.1.a)	informativa in merito a esatti termini e condizioni relative all'uso del servizio, compresa limitazione dell'uso		• Modulo di Adesione • Limiti d'uso e perimetro della soluzione

11	**DPCM** art 57.1.a)	subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente		• Modulo di Adesione • Identificazione e adesione alla modalità di firma [§ 4.2]
12	**DPCM** art 57.1.b)	conservare per almeno venti anni la dichiarazione di adesione al servizio		• conservazione documenti [§ 4.2]
13	**DPCM** art 57.1.b)	conservare per almeno venti anni la copia del documento di riconoscimento		• conservazione documenti [§ 4.2]
14	**DPCM** art 57.1.b)	conservare ogni altra informazione atta a dimostrare l'ottemperanza al **DPCM**		• conservazione documento elettronico con firma grafometrica
15	**DPCM** art 57.1.b)	utilizzare metodologie/strumenti di conservazione atte a garantire la disponibilità, l'integrità, la leggibilità e l'autenticità di dati e documenti		• sistema di conservazione elettronica a norma [§ 5.2.2]
16	**DPCM** art 57.1.c)	fornire liberamente copia della dichiarazione e le altre informazioni, su richiesta del firmatario		• procedura di richiesta dei documenti [§ 9.2]
17	**DPCM** art 57.1.d)	rendere note le modalità per richiedere copia della dichiarazione di adesione e le altre informazioni		• Procedura per la richiesta dei documenti [§ 9.2]
18	**DPCM** art 57.1.e)	rendere note le caratteristiche dei sistema realizzato		• Soluzione tecnologica [§ 4.2]
19	**DPCM** art 57.1.f)	specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto		• Soluzione tecnologica [§ 4.2]
20	**DPCM** art 57.1.g)	pubblicare le caratteristiche sul sito web		• Pubblicazione del Documento riassuntivo delle caratteristiche del servizio sul sito web www.sara.it
21	**DPCM** art 57.1.h)	assicurare ove possibile, la disponibilità di un servizio di revoca del consenso all'uso della FEA		• Revoca del consenso da parte del cliente [§ 8.1]
22	**DPCM** art 57.1.h)	assicurare la disponibilità di un servizio di assistenza		• Contatto per assistenza [§ 9.1]
23	**DPCM** art 57.2	gli erogatori della soluzione si dotano di una copertura assicurativa RC		• Assicurazione obbligatoria [§ 3.2]
24	**DPCM** art 57.3	Pubblicazione sul sito web delle informazioni sulla copertura assicurativa		• Pubblicazione del Documento riassuntivo delle caratteristiche del servizio sul sito web www.sara.it
28	**DPCM** art 60	limite di utilizzo della FEA nell'ambito dei rapporti giuridici tra sottoscrittore e soggetto erogatore		• Limite d'utilizzo dettagliato nel Modulo di Adesione e al