Manuale Operativo

Manuale Operativo Firma

Elettronica Avanzata FEA

Data	Gennaio 2023
Versione	3

1 Sommario

1. Premessa 5

Definizioni riguardanti i soggetti 6

1.1 Acronimi 6

2 Normativa 8

3 Scopo Del Documento 9

4 Attori del progetto 9

4.1 Soggetto erogatore 10

4.2 Soggetto Realizzatore 11

4.3 Soggetto Richiedente 11

5 Processi di identificazione utilizzati nella Soluzione 11

5.1 De visu 11

5.2 Self ID 11

6 Limite D'uso 12

7 La Soluzione SARA 12

7.1 Controllo del sistema di sottoscrizione 12

7.2 Strumenti per il controllo del sistema 13

8 La firma e la connessione univoca della firma al Firmatario 13

9 Conservazione Documenti 14

10 Cessazione del Servizio 15

10.1 Revoca del consenso da parte del Firmatario 15

10.2 Dismissione del servizio FEA 15

11 Tutela Assicurativa 15

12 Richiesta documentazione 16

1. Premessa

Il presente documento riporta le informazioni relative al progetto di F.E.A. (Firma Elettronica Avanzata) realizzato dalla società Sara Assicurazioni SpA con sede legale in Via Po, 20 - 00198 Roma, Codice fiscale 00408780583, Partita IVA 00885091009 e Sara Vita Spa con sede legale in Via Po, 20 - 00198 Roma, Codice fiscale 00408780583, Partita IVA 00885091009

(di seguito ciascuna denominata “SARA”)

Definizioni riguardanti i soggetti

Soggetto	Descrizione
Certificatore	È l'ente, pubblico o privato, abilitato a rilasciare certificati digitali previa specifica procedura di certificazione in conformità con gli standard nazionali ed europei.
Operatore	Persona incaricata, dal Soggetto che eroga i servizi di Firma Elettronica Avanzata, all'identificazione del Firmatario; lo informa in merito alle condizioni d'uso e alle modalità del servizio;
Soggetti erogatori dei servizi di firma elettronica avanzata	Soggetti giuridici che erogano soluzioni di firma elettronica avanzata al fine di utilizzarle nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali, realizzandole in proprio o anche avvalendosi di soluzioni realizzate dai soggetti che le realizzano come attività di impresa.
Soggetti realizzatori dei servizi di firma elettronica avanzata	Soggetti giuridici che, quale oggetto dell'attività di impresa, realizzano soluzioni di firma elettronica avanzata a favore di Soggetti erogatori.
Cliente, Firmatario, Richiedente	Soggetto a favore del quale la licenziataria mette a disposizione una soluzione di firma elettronica avanzata al fine di sottoscrivere i documenti informatici.

1.1 Acronimi

Sigle	Descrizione
AES	Advanced Encryption Standard è un algoritmo di cifratura a blocchi e a chiave simmetrica operante su un gruppo di bit a lunghezza finita.
AgID	Agenzia per l'Italia Digitale che, come da Decreto Legislativo 22 giugno 2012 n.83 articolo 22, ha sostituito CNIPA e DigitPa
CAD	Il codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n.82 e successive modificazioni.
Certificato digitale	Documento crittografico contenente i dati identificativi dell'intestatario e la sua chiave pubblica firmato dall'autorità di certificazione che attesta tali dati effettuando l'identificazione del soggetto.

Certificato qualificato	Il certificato digitale 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.
CNIPA (DigitPA)	Centro Nazionale per l'Informatica nella Pubblica Amministrazione. È l'organismo di controllo istituito dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri.

Sigle	Descrizione
Documento Informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
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.
Firma Elettronica Avanzata (FEA)	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.
Firma digitale	Particolare tipo di firma elettronica basata su un certificato e su un sistema di chiavi crittografiche, pubblica e privata, correlate tra loro, consentendo al titolare, tramite chiave privata, e al destinatario, tramite chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di uno o un insieme di documenti informatici.
Modulo di adesione	Documento contrattuale elaborato da Sara che raccoglie i consensi del Firmatario in merito all'utilizzo del sistema di firma elettronica avanzata, stipulato dal Firmatario una tantum all'inizio del rapporto o in un momento successivo
Responsabile della conservazione	Soggetto responsabile del sistema di conservazione dei documenti

Sigle	Descrizione
PAdes	Formato di busta crittografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modifiche.
PDF	È uno standard aperto per lo scambio di documenti elettronici incluso nella categoria ISO (International Organization for Standardization).

Soluzioni di firma elettronica avanzata	Soluzioni strumentali alla generazione e alla verifica della firma elettronica avanzata di cui all'art. 1, comma 1, lettera q-bis del DL 235/2010

2 Normativa

Riferimento	Descrizione
Regolamento Ue 910/2014	Rego. (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
DPR n. 445/2000	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.
Regolamento 679/2016	Regolamento EU relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
D.Lgs. 82/2005	Decreto Legislativo 7 marzo 2005 N. 82 "Codice dell'amministrazione Digitale".
DPCM 22 febbraio 2013	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,
Determinazione AgID n. 121/2019	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."
D. lgs. 231/2007	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".
Provvedimento di Banca d'Italia del 30 luglio 2019	Provvedimento recante Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio 08/07/2020 4/24 e del finanziamento del terrorismo la, ai sensi dell'art. 7, comma 2, del Decreto Legislativo 21 novembre 2007, n. 231.
Deliberazione CNIPA n. 11 del 19 febbraio 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.
Determinazione AgID n. 407/2020	Determinazione AgID n. 407/2020 recante - Linee guida sulla formazione, gestione e conservazione dei documenti informatici, modificate dalla Determinazione AgID n. 371/2021

3 Scopo Del Documento

Questo documento si pone lo scopo di descrivere le caratteristiche, le modalità operative, le procedure adottate e utilizzate da SARA al fine di gestire i servizi di Firma Elettronica Avanzata.

La "firma elettronica avanzata" (FEA) è stata introdotta nel nostro ordinamento dal decreto legislativo 30 dicembre 2010, n. 235 di modifica del CAD ed è oggi definita dall'art. 3, 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

4 Attori del progetto

4.1 Soggetto erogatore

Sara Assicurazioni S.p.A. e Sara Vita (di seguito "SARA" o "Soggetto erogatore") acquisiscono il ruolo, ognuno nei confronti dei propri Firmatari, di 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 SARA dai propri operatori o per mezzo della soluzione Self ID, nel rispetto della procedura di identificazione definita a validata dalla stessa. 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 sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente. Ai sensi dell'articolo 57 comma 2 del DPCM SARA ha stipulato una idonea copertura assicurativa per la responsabilità civile, nel rispetto dei massimali previsti dal DPCM. SARA si impegna nel rispetto del DPCM a svolgere le seguenti attività:

- Identificare in modo certo l'utente tramite un valido documento di riconoscimento;
- Informare l'utente in relazione agli esatti termini e condizioni d'uso del servizio, compresa ogni eventuale limitazione d'uso;

- Subordinare l'attivazione del servizio all'accettazione dell'informativa privacy e alla sottoscrizione del modulo di adesione contenente dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;

- Conservare per almeno 20 anni copia del documento di riconoscimento, modulo di adesione e informativa privacy;

- Garantire la disponibilità, integrità, leggibilità e autenticità del documento di accettazione del servizio;

- Rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dalle Regole Tecniche articolo 56, comma 1;

- Specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto;

- Prevedere la possibilità di revoca del servizio da parte del Firmatario/utente.

4.2 Soggetto Realizzatore

Intesa S.p.A. (di seguito "Intesa") è il soggetto Realizzatore della soluzione di FEA, come definito dall'articolo 55 comma 2 lettera b) del DPCM che eroga i servizi di OTP grazie alla propria piattaforma. Intesa 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 a norma. Per maggiori informazioni si rimanda al sito https://www.intesa.it/

Il Soggetto Realizzatore è tenuto a garantire che:

- la soluzione di firma (grafometrica o OTP) sviluppata sia conforme alle specifiche tecniche e funzionali definite con SARA;
- la soluzione tecnologica sviluppata consente la connessione univoca della firma al sottoscrittore e garantisca il controllo esclusivo del sottoscrittore del sistema di generazione della firma, ivi inclusi i codici identificativi inoltrati al Firmatario tramite SMS;
- Il documento informatico non possa subire modifiche dopo l'apposizione della firma.

4.3 Soggetto Richiedente

Soggetto Richiedente è il Firmatario che sottoscrive la documentazione contrattuale avvalendosi delle firme elettroniche. Il Richiedente è tenuto a garantire:

- la correttezza e la completezza dei dati personali forniti al soggetto erogatore, incluso il corretto recapito telefonico per utilizzo della firma OTP;
- la consegna o l'upload all'operatore o sulla soluzione Self ID di un documento di identità in corso di validità;
- di aver preso visione della documentazione descrittiva del servizio FEA prima dell'adesione al servizio.

5 Processi di identificazione utilizzati nella Soluzione

Il processo di identificazione del soggetto Firmatario può essere svolto nelle seguenti modalità:

5.1 De visu

Il processo di identificazione del soggetto Firmatario si concretizza nelle seguenti attività:

- l'operatore raccoglie il documento di identità (che deve essere conservato per 20 anni come previsto dall'articolo 57 comma 1 lettera b) del DPCM) del Firmatario e ne verifica le informazioni;
- l'operatore acquisisce copia per immagine del documento di identità;
- l'operatore mostra a video sul monitor o tablet (iPad) il modulo di adesione e il Manuale Operativo;
- il Firmatario è invitato a leggere su monitor o tablet (iPad) il presente Manuale Operativo nonché il modulo di adesione Fea. Il Modulo di adesione Fea (che riporta la descrizione del servizio e richiede esplicito consenso alla sottoscrizione in formato digitale della documentazione contrattuale) dovrà essere sottoscritto mediante un codice OTP ricevuto sul proprio mobile

5.2 Self ID e firma modulo di adesione

Il processo di identificazione del soggetto Firmatario si concretizza nelle seguenti attività:

- Il Firmatario accede alla piattaforma del Self ID
- Il Firmatario fa l'Upload del documento di identità (che deve essere conservato per 20 anni come previsto dall'articolo 57 comma 1 lettera b) del DPCM). Può essere utilizzato 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.
- Certificazione dispositivo mobile e dell'indirizzo e-mail mediante codice OTP
- Il Firmatario su apposita guida della piattaforma dovrà svolgere dei movimenti randomici del volto (Check Liveness)
- La piattaforma scatterà una foto del volto del Firmatario al fine di effettuare il face matching tra la foto del documento caricato e il selfie scattato.
- Completato il processo di identificazione verrà mostrato il modulo di adesione Fea (che riporta la descrizione del servizio e richiede esplicito consenso alla sottoscrizione in formato digitale della documentazione contrattuale e all'interno del quale c'è un collegamento attraverso il quale è possibile accedere al presente Manuale Operativo) che dovrà essere sottoscritto mediante un codice OTP ricevuto sul proprio mobile. Il modulo di adesione contenente la dichiarazione di adesione ai servizi di firma elettronica avanzata, potrà essere scaricato dal Firmatario affinché questo possa leggerlo. 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 Firmatario e pertanto non sarà necessaria ulteriore adesione in fase di firma dei successivi singoli documenti contrattuali. Dopo l'apposizione delle firme il modulo così sottoscritto viene inviato via mail all'indirizzo e-mail fornito dal

Firmatario.

Processo sospeso

In caso di sospensione del processo (processi non terminati, abbandonati o interrotti per motivi tecnici, OTP fallito, problemi di rete, etc.) interverrà un operatore del Customer Center (CC) di SARA che potrà seguire le seguenti strade:

- 1a. Se il Firmatario manifesta la volontà di proseguire e il link risulta ancora attivo, l'operatore potrà re-inviare un nuovo link di accesso alla piattaforma Intesa ('**Re-send link riconoscimento**').

- 1b. Se il Firmatario manifesta la volontà di proseguire, ma il link risulta scaduto oppure la verifica OTP è bloccata, l'operatore potrà inviare un nuovo link di accesso alla piattaforma Intesa, ('**Re-start riconoscimento**'). La precedente sessione sarà distrutta automaticamente da Intesa allo scadere del tempo massimo previsto.

- 1c. Se il Firmatario manifesta la volontà di cambiare il numero di cellulare, l'operatore dovrà richiedergli di aprire un case di 'Modifica Dati' da app/hi oppure, se non ancora registrato in HI, di contattare direttamente l'agenzia di riferimento. Una volta aggiornato il cellulare l'agente potrà utilizzare la funzionalità descritta nel punto precedente ('**Re-start riconoscimento'**) per inviare al Firmatario un nuovo link di accesso. La precedente sessione sarà distrutta automaticamente da Intesa allo scadere del tempo massimo previsto.

Processo bloccato

In caso di riconoscimento fallito (per liveness o facematch negativo) l'operatore del CC riceverà un case, tramite il case farà accesso alla console Intesa e utilizzerà la voce di menu '**Processi In Corso**' ricercando per nominativo/codice fiscale. Potrà consultare i documenti, confrontarli con il video registrato e recuperare i contatti del Firmatario per richiamarlo.
L'operatore richiede al Firmatario di recarsi in agenzia per maggiori verifiche.
L'agente potrà accedere alla scheda di Firmatario, utilizzando la stessa funzionalità di cui al punto precedente, confermare il riconoscimento in presenza. L'azione determinerà l'invio via mail al Firmatario del link per procedere alla firma della documentazione contrattuale tramite Docusign).

5.3 Self onboarding tramite credenziali SPID e firma modulo di adesione

Il processo di identificazione del soggetto Firmatario si concretizza nelle seguenti attività:

- Il Firmatario accede alla piattaforma di riconoscimento
- Il Firmatario acconsente all'emissione di un certificato qualificato di firma elettronica per la sottoscrizione dell'informativa privacy di Intesa che verrà restituito a SARA quale conferma della verifica dell'identità del Firmatario stesso;
- Il Firmatario clicca "Entra con SPID" e si autentica con il proprio Identity Provider tramite le credenziali

SPID di livello 2 o superiore

- Il Firmatario conferma la trasmissione dei dati recepiti
- Intesa emette il certificato di firma qualificato e appone la firma sul documento privacy summenzionato inviandolo corredato dei dati anagrafici del Firmatario a SARA
- Certificazione dispositivo mobile e dell'indirizzo e-mail mediante codice OTP
- Completato il processo di identificazione verrà mostrato il modulo di adesione Fea (che riporta la descrizione del servizio e richiede esplicito consenso alla sottoscrizione in formato digitale della documentazione contrattuale e all'interno del quale c'è un collegamento attraverso il quale è possibile accedere al presente Manuale Operativo) che dovrà essere sottoscritto mediante un codice OTP ricevuto sul proprio mobile. Il modulo di adesione contenente la dichiarazione di adesione ai servizi di firma elettronica avanzata, potrà essere scaricato dal Firmatario affinché questo possa leggerlo. Il modulo di adesione così firmato, l'evidenza informatica della verifica dell'identità e il documento di identità raccolto da SARA sono conservati a norma per almeno 20 anni. L'adesione vale fino a successiva eventuale revoca del Firmatario e pertanto non sarà necessaria ulteriore adesione in fase di firma dei successivi singoli documenti contrattuali. Dopo l'apposizione delle firme il modulo così sottoscritto viene inviato via mail all'indirizzo e-mail fornito dal Firmatario.

6 Limite D'uso

Il DPCM 22 febbraio 2013, prevede per la Firma Elettronica Avanzata le seguenti limitazioni:

- Non è consentito il libero scambio di documenti informatici: il suo uso è limitato al contesto;
- La FEA è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il Firmatario e il soggetto che eroga soluzioni di FEA
- Articolo 21 del CAD prevede che le scritture private di cui all'art. 1350, comma 1 da n. 1 a 12 c.c., se formate su documento informatico, sono sottoscritte, a pena di nullità, soltanto con firma digitale o qualificata; invece le scritture di cui all'art. 1350, comma 1 n. 13 possono essere sottoscritte anche con firma elettronica avanzata.

7 La Soluzione SARA

La postazione dell'operatore e la piattaforma Self ID colloquiano con la piattaforma di firma OTP erogata da Intesa, a Kyndryl Company, 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
- marcatura temporale del documento a validazione dell'istante di firma;
- restituzione del documento firmato alle applicazioni di SARA.

Il cellulare del Firmatario è lo strumento certificato in fase di adesione al servizio di firma OTP ed abilitato a ricevere, mediante SMS, il codice da utilizzare per sottoscrivere i documenti contrattuali.

7.1 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 elettronica avanzata OTP.

7.2 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.

Tra i sistemi evoluti per il controllo dell'intero sistema a maggior tutela degli utenti vi sono anche sistemi di protezione contro gli eventi catastrofici quali:

- protezione contro gli incendi;
- protezione contro gli allagamenti;

8 La firma e la connessione univoca della firma al Firmatario

Come noto, la definizione di firma elettronica avanzata è tecnologicamente neutra e la norma non richiede e non impone l'uso di una determinata tecnologia.

La firma elettronica avanzata, infatti, rappresenta una particolare specie di firma elettronica con alcune peculiari caratteristiche di sicurezza che si riscontrano pienamente nella soluzione denominata Firma OTP implementata da SARA.

Più precisamente la soluzione implementata da SARA in conformità con l'Art. 26 del Regolamento eIDAS soddisfa i seguenti requisiti:

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; e
d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

Grazie alla tecnologia utilizzata è garantito al Firmatario un processo sicuro e verificabile. Infatti tramite l'invio

di un codice OTP ad un numero di cellulare verificato, il Servizio implementato è in grado di associare in maniera univoca il Firmatario alla firma elettronica che viene raccolta nel processo implementato.

La Firma OTP garantisce pienamente il rispetto di queste due condizioni attraverso l'impiego di un codice (parliamo proprio dell'OTP) comunicato in maniera riservata al Firmatario.

Proprio l'inserimento dell'OTP ricevuto sul cellulare precedentemente registrato è uno dei punti qualificanti di tutto il processo.

Il cellulare si può considerare a tutti gli effetti come il dispositivo di sicurezza abilitante alla firma.

Infatti, la firma del documento può essere ricondotta alla volontà del Firmatario che ha ricevuto un OTP per sottoscrivere il documento.

Il Firmatario è inoltre informato che la sottrazione, il furto, l'appropriazione indebita, lo smarrimento o l'uso non autorizzato del mobile in quanto dispositivo di sicurezza deve essere immediatamente comunicato.

La procedura, infatti, non consente l'invio al Firmatario di un OTP ad un numero di cellulare che non sia stato precedentemente certificato nell'Anagrafica Firmatario. Quindi nel caso anche di semplice sostituzione del cellulare si dovrà prima procedere con la registrazione del nuovo numero secondo le politiche previste da Sara e solo al termine delle stesse avviare il processo di firma.

Una sostituzione "al volo" del numero di cellulare a cui inviare l'OTP non è invece prevista in alcun caso, ritenendo questa procedura pericolosa e non sicura contro un eventuale tentativo di furto d'identità (un soggetto diverso dal Firmatario che cerca di fornire un proprio numero telefonico dopo essere entrato in qualche maniera in possesso dell'e-mail del destinatario originale).

La Riconducibilità del documento informatico alla volontà del Firmatario è garantita poi da un insieme di dati incapsulati nella firma del documento (di seguito "Summary o Certificato di Completamento").

Nel Certificato di Completamento vengono registrate tutte le principali attività legate alla vita del documento e alla firma per permettere poi in qualsiasi momento la verifica dello stesso.

Per ogni documento il sistema genera automaticamente e memorizza, marcandola temporalmente, la storia completa di ogni invio, visualizzazione, stampa, firma o azione di rigetto/rifiuto.

Qualsiasi parte coinvolta nel processo che vuole rivedere l'attività associata ad un documento è in grado di visualizzare, scaricare o stampare il Certificato di Completamento associato al documento dopo che questo sia stato firmato.

A ulteriore garanzia sull'integrità del documento firmato e del Certificato di Completamento associato il sistema protegge tali informazioni con dei sistemi anticontraffazione utilizzando dei processi che fanno uso di tecnologia PKI (Public Key Infrastructure) di fatto controfirmando con una sorta di sigillo tutti i documenti oggetto della transazione.

Tale insieme di dati è creato grazie a mezzi dei quali il Firmatario ha un controllo esclusivo (in particolare il numero di cellulare). Il Certificato di Completamento contiene, poi, tutte le informazioni che garantiscono la connessione univoca al documento e il collegamento logico tra il documento stesso e il soggetto a cui è ascrivibile la firma.

Tali dati garantiscono il completo rispetto del requisito con elevati standard di sicurezza.

9 Conservazione Documenti

In pieno rispetto di quanto previsto dall'art. 56 comma 1 del DPCM 22/02/2013 si esegue copia del documento di riconoscimento. Queste copie, in allegato al modulo di adesione Fea, verranno conservate per almeno 20, anni, garantendo per tutto il periodo la disponibilità, integrità e leggibilità.

10 Cessazione del Servizio

L'erogazione del servizio di firma elettronica avanzata può essere interrotta per revoca del consenso da parte del Firmatario o per dismissione del servizio da parte di SARA. Si illustrano di seguito gli effetti dei due casi di cessazione.

10.1 Revoca del consenso da parte del Firmatario

In caso il Firmatario scelga di revocare il proprio consenso all'utilizzo del servizio di FEA, i documenti che regolano i rapporti tra il Firmatario e le società dovranno essere sottoscritti mediante firma autografa su carta. Restano salvi i documenti precedentemente sottoscritti con firma elettronica avanzata. La revoca potrà essere effettuata anche nei confronti di uno solo dei Soggetti Erogatori, mantenendo valida l'adesione solo per i servizi erogati dal Soggetto Erogatore non interessato dalla revoca.

La revoca del consenso deve essere esercitata mediante comunicazione scritta con oggetto "REVOCA ADESIONE FEA" all'Agenzia Sara a cui il Firmatario viene assegnato all'indirizzo e-mail, indicato nella comunicazione di conferma dell'acquisto.

In alternativa il Firmatario potrà manifestare la propria volontà di revoca inviando apposita comunicazione con oggetto "REVOCA ADESIONE FEA" a mezzo raccomandata all'indirizzo Sara assicurazioni SPA via Po 20 00198 Roma ovvero, ancora, via PEC all'indirizzo saraassicurazioni@sara.telecompost.it o rispettivamente a Sara Vita Spa via Po, 20 00198 - Rom asaravita@sara.telecompost.it

10.2 Dismissione del servizio FEA

Qualora SARA decidesse di dismettere il servizio di FEA, i documenti che regolano i rapporti tra il Firmatario e le società saranno sottoscritti mediante firma autografa su carta o con altre modalità ad esempio firme digitali.

Restano salvi i documenti precedentemente sottoscritti con firma elettronica avanzata che continueranno ad essere conservati a norma per tutto il termine di conservazione previsto. SARA continuerà a conservare inoltre il Modulo di adesione alla Fea e la copia del documento di identità del Firmatario fino alla scadenza del termine ventennale di conservazione previsto dal DPCM per il Soggetto Erogatore.

11 Tutela Assicurativa

Sara Assicurazioni ha stipulato una idonea copertura assicurativa per la responsabilità civile in conformità all'art 57 comma 2 del DPCM che recita quanto segue:

“Il soggetto che eroga soluzioni di Firma Elettronica Avanzata si impegna a stipulare una polizza assicurativa, con società abilitata ad esercitare nel campo dei rischi industriali, per la copertura dei rischi dell’attività svolta e dei danni a tutela delle parti (Firmatari ed i Terzi) per almeno Euro 500.000,00(cinquecentomila/00).”

12 Richiesta documenti

Il Firmatario 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 elettronica avanzata. I documenti vanno richiesti direttamente a all’Agenzia Sara a cui il Firmatario viene assegnato all’indirizzo e-mail, indicato nella comunicazione di conferma dell’acquisto, che provvederà a fornirli al Firmatario inviandoli via mail all’indirizzo e-mail fornito dal Firmatario. I documenti sono forniti sotto forma di copia per immagine non contenente i dati biometrici per ragioni di sicurezza. 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 Firmatario può chiedere a Sara l’esibizione della documentazione in originale. I documenti sono forniti al richiedente seguendo le disposizioni del Garante della Privacy.