MANUALE TECNICO
DELLA SOLUZIONE DIFIRMA ELETTRONICA AVANZATA (FEA)

REGISTRO DELLE VERSIONI

N° Versione	Data emissione
1.1	12.07.2019
1.2	17.04.2026

Sommario

1. DEFINIZIONE GENERALE DELLA FEA 3
2. GLOSSARIO 3
3. RIFERIMENTI NORMATIVI 5
4. AMBITO E SCOPO DEL DOCUMENTO 6
5. ATTORI COINVOLTI 6
6. OBBLIGHI DEGLI ATTORI 8
7. LIMITI D'USO E PERIMETRO DELLA SOLUZIONE 9
8. CARATTERISTICHE GENERALI DELLA SOLUZIONE FEA 10
   - 8.1 GARANZIE DEI REQUISITI DELLA SOLUZIONE FEA 10
   - 8.2 TIPOLOGIE DI SOLUZIONI FEA 10
9. CARATTERISTICHE ANALITICHE DELLA SOLUZIONE FEA 11
   - 9.1 ADESIONE ALL'UTILIZZO DELLA SOLUZIONE FEA 11
   - 9.2 IDENTIFICAZIONE DEL FIRMATARIO 11
   - 9.3 CONNESSIONE UNIVOCA DELLA FIRMA AL FIRMATARIO 11
   - 9.4 CONTROLLO ESCLUSIVO DEL FIRMATARIO DEL SISTEMA DI GENERAZIONE DELLA FEA 12
   - 9.5 POSSIBILITÀ DI VERIFICA CHE IL DOCUMENTO INFORMATICO SOTTOSCRITTO NON ABBIA SUBITO MODIFICHE DOPO L'APPOSIZIONE DELLA FIRMA 13
   - 9.6 POSSIBILITÀ PER IL FIRMATARIO DI OTTENERE EVIDENZA DI QUANTO SOTTOSCRITTO 13
   - 9.7 INDIVIDUAZIONE DEL SOGGETTO EROGATORE DELLA SOLUZIONE FEA 13
   - 9.8 ASSENZA NELL'OGGETTO DELLA SOTTOSCRIZIONE DI QUALUNQUE ELEMENTO IDONEO A MODIFICARNE GLI ATTI, I FATTI E I DATI IN ESSO RAPPRESENTATI 14
   - 9.9 CONNESSIONE UNIVOCA DELLA FIRMA AL DOCUMENTO SOTTOSCRITTO 14
   - 9.10 OPERAZIONE DI GENERAZIONE, CONSEGNA E CONSERVAZIONE DELLA CHIAVE DI CRIPTAZIONE 14
   - 9.11 VERIFICA DELL'AUTENTICITÀ DELLA FEA 15
   - 9.12 LA SICUREZZA DELLA FEA REALIZZATA DAL SOGGETTO EROGATORE 15
   - 9.13 CERTIFICAZIONE ISO/IEC 27001 DEL PRODUTTORE DELLA TECNOLOGIA FEA 16
   - 9.14 LA DESCRIZIONE DELLA COPERTURA ASSICURATIVA 17
   - 9.15 MODALITÀ DI RICHIESTA ASSISTENZA E COPIA DEL MODULO DI ADESIONE FEA 17
   - 9.16 LA REVOCA DALLA SOLUZIONE FEA 17
   - 9.17 REQUISITI DELLA SOLUZIONE FEA AI SENSI DELL'ART. 56 DEL DPCM 17
   - 9.18 CONSERVAZIONE A NORMA DEI DOCUMENTI SOTTOSCRITTI 18

1. DEFINIZIONE GENERALE DELLA FEA

La Firma Elettronica Avanzata (nel seguito "FEA") è una firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati

Più nel dettaglio, la FEA è un processo di firma elettronica con dei requisiti disciplinati dal **titolo V del DPCM 22 febbraio 2013** "*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali*" pubblicate in Gazzetta Ufficiale n. 117 del 21.05.2013 (nel seguito "DPCM"), attuative del Codice dell'Amministrazione Digitale (decreto legislativo 07.03.2005, n. 82, e successive modificazioni).

In particolare, l'art. 56 comma 1 del DPCM richiede che la soluzione FEA garantisca:
a) l'identificazione del firmatario del documento;
b) la connessione univoca della firma al firmatario;
c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma;
d) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
f) l'individuazione del soggetto che ha erogato la soluzione di firma elettronica avanzata;
g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;

Se la FEA soddisfa quanto predetto, allora assicura l'identità dell'autore (del firmatario), l'integrità e l'immodificabilità del documento informatico sottoscritto, garantendo il **requisito della forma scritta** e **l'efficacia probatoria** prevista dall'art. 2702 del Codice Civile.

Torna al sommario

2. GLOSSARIO

I termini di seguito elencati sono utilizzati nel presente documento con il significato qui indicato. Per i termini definiti dal CAD e dal DPCM si rimanda alle definizioni in essi stabilite.

Termine	Definizione
Certificato di firma elettronica	Attestato elettronico che associa i dati di convalida di una firma elettronica a una persona fisica, confermandone almeno il nome o lo pseudonimo.
Chiave privata	Elemento della coppia di chiavi asimmetriche utilizzato dal firmatario per generare la firma elettronica sul documento informatico.

Chiave pubblica	Elemento della coppia di chiavi asimmetriche reso pubblico, tramite il quale è possibile verificare la firma elettronica apposta dal firmatario.
Convalida	Processo di verifica e conferma della validità di una firma elettronica.
Conservazione	Archiviazione sicura a lungo termine di documenti informatici che ne assicura integrità, disponibilità e mantenimento del valore legale nel tempo.
Documento elettronico	Qualsiasi contenuto conservato in formato elettronico, inclusi testo, registrazioni sonore, visive o audiovisive.
Firma digitale	Tipo particolare di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche asimmetriche.
Firma elettronica	Dati in formato elettronico, acclusi o connessi tramite associazione logica ad altri dati elettronici, utilizzati dal firmatario per apporre la propria sottoscrizione.
Firma Elettronica Avanzata (FEA)	Firma elettronica che soddisfa i requisiti di cui all'articolo 26 del Regolamento eIDAS e al Titolo V del DPCM 22 febbraio 2013.
Firma Elettronica Qualificata (FEQ)	Firma elettronica avanzata generata mediante un dispositivo qualificato per la creazione di firme elettroniche e basata su un certificato qualificato.
Firmatario	Persona fisica che appone una firma elettronica.
Hash / Impronta	Sequenza di bit di lunghezza predefinita generata dall'applicazione di una funzione matematica a un'evidenza informatica, ai sensi dell'art. 1, co. 1, lett. h DPCM.
OTP (One-Time Password)	Codice di autenticazione monouso, generato e reso disponibile al firmatario immediatamente prima dell'apposizione della firma elettronica.
Soggetto Erogatore	Soggetto che eroga la soluzione di Firma Elettronica Avanzata ai sensi dell'art. 55 del DPCM 22 febbraio 2013.
Soggetto Realizzatore	Soggetto che realizza la soluzione di Firma Elettronica Avanzata ai sensi dell'art. 55 del DPCM 22 febbraio 2013.
Validazione temporale elettronica	Dati in formato elettronico che collegano altri dati elettronici a una particolare data e ora, attestandone l'esistenza in quel momento.

3. RIFERIMENTI NORMATIVI

Nella predisposizione della soluzione di Firma Elettronica Avanzata si è fatto riferimento alle seguenti fonti normative e tecniche:

- [1] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio (eIDAS) in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno;
- [2] Decreto Legislativo 7 marzo 2005, n. 82 (G.U. n. 112 del 16 maggio 2005) – Codice dell'Amministrazione Digitale (CAD) e successive modifiche e integrazioni;
- [3] Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 (G.U. n. 117 del 21 maggio 2013) – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali;
- [4] Decreto del Presidente del Consiglio dei Ministri 13 novembre 2014 (G.U. n. 8 del 12 gennaio 2015) – Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici;
- [5] Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 (G.U. n. 59 del 12 marzo 2014) – Regole tecniche in materia di sistema di conservazione;
- [6] D.P.R. 28 dicembre 2000, n. 445 (G.U. n. 42 del 20 febbraio 2001) – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.

4. AMBITO E SCOPO DEL DOCUMENTO

Il presente documento ha lo scopo di fornire al Cliente della Piattaforma Hub, denominata TeamSystem Digital, un manuale in cui sono descritte le caratteristiche tecnologiche della soluzione di Firma Elettronica Avanzata.

Il Cliente della piattaforma TeamSystem Digital di TeamSystem Service S.r.l. agisce in qualità di **Soggetto Erogatore**, ai sensi dell'art. 55, comma 1, lettera a) del DPCM, ossia il soggetto che implementa ed eroga la soluzione FEA allo scopo di consentire ai propri firmatari (nel seguito anche "**Utenti**") di sottoscrivere documenti informatici trattati **esclusivamente nell'ambito dei rapporti giuridici intercorrenti con il Soggetto Erogatore stesso**.

Il Soggetto Erogatore è individuato nel modulo di adesione al servizio di FEA che l'Utente sottoscrive prima di utilizzare la soluzione di Firma Elettronica Avanzata per la sottoscrizione dei documenti informatici.

Il Soggetto Erogatore ha il dovere di mettere a disposizione dell'Utente il presente manuale e renderlo disponibile anche su una pagina o sezione dedicata del sito internet per soddisfare i doveri di trasparenza informativa in ottemperanza all'art. 57, lett. e) ed f) del DPCM.

Il presente manuale è comunque pubblicato sul sito web della piattaforma Hub TeamSystem Digital.

Torna al sommario

5. ATTORI COINVOLTI

Soggetto Erogatore
Il Soggetto Erogatore è il cliente della piattaforma TeamSystem Digital che, nell'ambito dei propri rapporti con soggetti terzi, implementa e rende disponibile la soluzione di Firma Elettronica Avanzata ai propri utenti. Agisce ai sensi dell'art. 55, comma 1, lettera a) del DPCM quale soggetto responsabile dell'erogazione del servizio FEA, consentendo ai propri firmatari di sottoscrivere documenti informatici esclusivamente nell'ambito dei rapporti giuridici intercorrenti con il Soggetto Erogatore stesso.
I dati identificativi del Soggetto Erogatore sono riportati nel modulo di adesione al servizio di FEA che il firmatario sottoscrive prima di utilizzare la soluzione.

Soggetto Realizzatore
TeamSystem Service S.r.l. è il soggetto che, quale oggetto della propria attività d'impresa, sviluppa e realizza soluzioni di firma elettronica avanzata destinate ai Soggetti Erogatori mediante la piattaforma Hub denominata TeamSystem Digital. TeamSystem Service S.r.l. si avvale della sua tecnologia software certificata ISO/IEC 27001:2013 e del proprio sistema di gestione della sicurezza delle informazioni. Per la modalità con certificato one-shot, la tecnologia di emissione e gestione dei certificati è fornita dalla Certificate Authority Telecom Italia Trust Technologies S.r.l.

Utente / Firmatario
È la persona fisica che utilizza lo strumento di Firma Elettronica Avanzata al fine di perfezionare, modificare o estinguere i rapporti contrattuali con il Soggetto Erogatore, e/o dar corso alle relative

operazioni e comunicazioni. Il firmatario aderisce volontariamente alla soluzione FEA sottoscrivendo l’apposito modulo di adesione.

6. OBBLIGHI DEGLI ATTORI

Obblighi del Soggetto Erogatore

Il Soggetto Erogatore, in relazione al processo di Firma Elettronica Avanzata, è tenuto a garantire che:

• siano rispettate le regole tecniche stabilite dal DPCM [3];

• il firmatario sia preventivamente identificato tramite un valido documento di riconoscimento in corso di validità;

• il firmatario sia adeguatamente informato in merito ai termini, alle condizioni e alle limitazioni d'uso del servizio FEA prima dell'adesione;

• l'attivazione del servizio FEA sia subordinata alla sottoscrizione, da parte del firmatario, di una dichiarazione di accettazione delle condizioni d'uso;

• la copia del documento di riconoscimento e la dichiarazione di adesione siano conservate per almeno 20 anni, garantendone disponibilità, integrità, leggibilità e autenticità;

• il firmatario possa ottenere gratuitamente, su richiesta, copia della dichiarazione di adesione e di ogni informazione inerente la soluzione;

• siano rese pubbliche, anche tramite il proprio sito internet, tutte le informazioni prescritte dal DPCM [3], compreso il presente documento;

• sia reso disponibile al firmatario un servizio di revoca del consenso all'utilizzo della FEA;

• sia fornito al firmatario un servizio di assistenza;

• la FEA sia apponibile esclusivamente dal firmatario, con piena coscienza del documento oggetto di sottoscrizione;

• non sia possibile riutilizzare una sottoscrizione già apposta su un documento per un documento informatico differente.

Obblighi del Soggetto Realizzatore

Il Soggetto Realizzatore è tenuto a garantire che:

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

• il documento informatico non possa subire modifiche successive all'apposizione della firma.

Obblighi del Firmatario

Il firmatario è tenuto a garantire:

• la veridicità, correttezza e completezza dei dati personali forniti al Soggetto Erogatore;

• la consegna al Soggetto Erogatore di un documento di identità in corso di validità al momento della sottoscrizione del modulo di adesione;

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

7. LIMITI D'USO E PERIMETRO DELLA SOLUZIONE

Ai sensi dell'articolo 60 del DPCM [3], come dettagliato nel modulo di adesione al servizio, la Firma Elettronica Avanzata è utilizzabile esclusivamente nell'ambito dei rapporti giuridici intercorrenti tra il firmatario e il Soggetto Erogatore. L'utilizzo della soluzione FEA non può pertanto estendersi a rapporti con soggetti terzi diversi dal Soggetto Erogatore identificato nel modulo di adesione.
La sottoscrizione mediante FEA ha il medesimo valore giuridico della sottoscrizione autografa ai sensi dell'art. 2702 del Codice Civile, limitatamente ai documenti trattati nell'ambito del rapporto contrattuale tra firmatario e Soggetto Erogatore e nei limiti stabiliti dalla vigente normativa.
Il firmatario è tenuto a utilizzare la soluzione FEA unicamente per la sottoscrizione dei documenti esplicitamente proposti dal Soggetto Erogatore nell'ambito del predetto rapporto contrattuale, escludendo qualsiasi utilizzo al di fuori di tale perimetro.

8. CARATTERISTICHE GENERALI DELLA SOLUZIONE FEA

8.1 Garanzie dei requisiti della soluzione FEA

Il processo associato alla soluzione FEA erogata dal Soggetto Erogatore garantisce l'identificazione dell'Utente (firmatario), la connessione univoca della firma al firmatario, il controllo esclusivo del firmatario del sistema di generazione della FEA, la possibilità di verificare che il documento non abbia subito modifiche dopo l'apposizione della firma, la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto e l'individuazione del Soggetto Erogatore che realizza le soluzioni di FEA.

La soluzione di FEA è attuata dal Soggetto Erogatore nel rispetto delle vigenti disposizioni normative in materia di FEA e del trattamento dei dati personali (privacy), in particolare in conformità alle prescrizioni in materia di privacy dettate in tema di biometria dal Provvedimento n. 513 del 26.11.2014 del Garante per la Protezione dei Dati Personali.

8.2 Tipologie di soluzioni FEA

La soluzione di FEA messa a disposizione dal Soggetto Erogatore è strutturata in tre tipologie di soluzioni, distinte e alternative, che sono basate su tre differenti tecnologie:

- **FEA Grafometrica**: soluzione di FEA basata sull'espressione della volontà del firmatario di sottoscrivere il documento informatico mediante l'apposizione di una firma con una penna elettronica su tavolette di acquisizione o dispositivi tablet (denominati nel seguito "signature pad") equipaggiati con opportuni sensori e software, che acquisiscono i dati grafometrici connessi alla firma autografa del sottoscrittore (quali ritmo, pressione, velocità, accelerazione e movimento), incapsulati in forma criptata nel documento informatico stesso.

- **FEA in Mobilità**: soluzione di FEA basata sull'espressione della volontà del firmatario di sottoscrivere il documento informatico mediante un processo combinato di "point and click" e di successiva conferma della transazione mediante inserimento di una OTP (one-time-password), *(i)* tramite una chiamata a un numero verde dedicato attraverso una SIM card, della quale il firmatario dichiara e garantisce di avere la piena ed esclusiva disponibilità, ovvero *(ii)* tramite sms alla predetta Sim card del firmatario, ovvero *(iii)* tramite OTP generato da apposita applicazione installata sullo smartphone del firmatario di cui il firmatario dichiara e garantisce di averne la piena ed esclusiva disponibilità.

- **FEA con certificato one-shot**: soluzione di FEA basata sull'espressione della volontà del firmatario di sottoscrivere il documento informatico mediante un processo combinato di "point and click" e di successiva conferma della transazione mediante inserimento di una OTP (one-time-password). La connessione univoca della firma al documento sottoscritto è garantita dall'apposizione al documento stesso di un certificato digitale non qualificato di tipo one-shot (usa e getta), emesso da una Certificate Authority (CA) privata a nome del firmatario.

9. CARATTERISTICHE ANALITICHE DELLA SOLUZIONE FEA

Di seguito sono descritte analiticamente le caratteristiche della soluzione FEA adottata in relazione ai requisiti richiesti dalla norma, con l'approfondimento, ove necessario, sulle specifiche caratteristiche delle due tipologie di soluzioni FEA.

9.1 Adesione all'utilizzo della soluzione FEA

L'adesione alla soluzione FEA è facoltativa e può essere revocata in qualsiasi momento dall'Utente. Laddove l'Utente firmatario non ne accettasse le condizioni, in ogni loro parte, il processo di sottoscrizione dei documenti viene comunque realizzato in modalità tradizionale cartacea.
L'Utente per utilizzare la soluzione FEA deve obbligatoriamente essere identificato e preventivamente prestare la propria adesione firmando l'apposito modulo di adesione del Soggetto Erogatore che dettaglia le modalità di fruizione della soluzione FEA (comprese le limitazioni d'uso) nonché il trattamento dei dati personali effettuato nell'erogazione del servizio di sottoscrizione.

L'utente firmatario, attraverso la sottoscrizione del modulo di adesione, manifesta la volontà di aderire alla soluzione FEA e accetta la modalità di trattamento dei dati personali.

9.2 Identificazione del firmatario

Il Soggetto Erogatore identifica in modo certo l'Utente firmatario richiedendo il relativo documento d'identità (in corso di validità) e codice fiscale, di cui ne acquisisce copia in fase di adesione al servizio FEA. La copia del documento d'identità ed il modulo di adesione al servizio sottoscritto dal firmatario sono conservati per almeno 20 anni.

9.3 Connessione univoca della firma al firmatario

4.3.1 FEA Grafometrica

Il sistema registra, oltre ai dati relativi all'immagine grafica, anche le caratteristiche dinamiche della firma autografa che il firmatario appone di suo pugno con penna elettronica su un apposito dispositivo, il signature pad del Soggetto Erogatore. Le caratteristiche registrate corrispondono alla scansione temporale di posizione, ovvero il ritmo, la velocità e la pressione della penna, acquisite durante la firma sul signature pad. I dati grafometrici sono tipici e specifici di ogni persona. L'univocità della connessione viene quindi garantita dalla sottoscrizione effettuata davanti all'operatore del Soggetto Erogatore, previo riconoscimento del firmatario, e dalla acquisizione attraverso il signature pad, in sede di apposizione della firma, di dati comportamentali (c.d. biometrici) univocamente riconducibili al firmatario medesimo ed associati indissolubilmente al documento informatico da lui sottoscritto.

4.3.2 FEA in Mobilità

L’univocità della connessione della firma al firmatario, presupposto obbligatorio per la sottoscrizione del documento informatico, viene garantita dalla correlazione univoca via software dell’Utente firmatario, inizialmente riconosciuto mediante documento d'identità in corso di validità da parte di un operatore del Soggetto Erogatore, al processo di sottoscrizione, nonché dall’utilizzo da parte del firmatario di un numero di cellulare riferito ad una SIM card di cui dichiara di avere, in quel momento e per tutto l’arco temporale del processo di sottoscrizione, piena ed esclusiva disponibilità.

4.3.3 FEA con certificato one-shot

La connessione univoca della firma al documento sottoscritto è garantita dall’apposizione al documento stesso di un certificato digitale non qualificato di tipo one-shot (usa e getta), emesso da una Certificate Authority (CA) privata a nome del firmatario

9.4 Controllo esclusivo del firmatario del sistema di generazione della FEA

4.4.1 FEA Grafometrica

Durante la fase di firma, il sistema è nella piena ed esclusiva disponibilità, nonché sotto il controllo esclusivo del firmatario e sottoposto ai rigidi controlli di sicurezza elencati al punto 4.12.1.

Lo schermo del dispositivo di firma (signature pad) o del computer del Soggetto Erogatore mostra il dettaglio della condizione o clausola oggetto della firma consentendo al firmatario di verificare personalmente i propri dati ed il dettaglio della condizione. Durante l’apposizione della firma, il sistema guida il cliente nel processo di firma. Mentre egli appone la firma con l’apposita penna elettronica l’immagine della firma appare in tempo reale sul signature pad Apposite funzioni consentono al firmatario di confermare o cancellare la firma in caso di errori. Ogni comunicazione tra il signature pad e il sistema di generazione della firma è criptata ed anche i dati grafometrici relativi alla firma apposta sul signature pad dal firmatario sono automaticamente cifrati. A seguito della loro cifratura ed invio su canale criptato al server (per la gestione delle ulteriori fasi del processo), i dati grafometrici temporaneamente registrati nella memoria del signature pad sono eliminati e non sono più recuperabili.

4.4.2 FEA in Mobilità o con certificato one-shot

Durante la fase di firma, il sistema è nella piena ed esclusiva disponibilità nonché sotto il controllo esclusivo del firmatario e sottoposto ai rigidi controlli di sicurezza elencati al punto 4.12.2. Il firmatario dispone di un proprio computer o tablet, di cui ne ha la piena ed esclusiva disponibilità, sul quale ha la possibilità di verificare personalmente i propri dati ed ogni dettaglio sulla condizione o clausola da sottoscrivere, procede quindi in autonomia alla lettura delle clausole ed alla selezione dei relativi campi di firma sui quali il firmatario è chiamato ad esprimere manualmente (processo di "point and click") la propria volontà di sottoscrizione.

Dopo la conferma:

- Il computer o tablet visualizza un numero telefonico (numero verde con chiamata gratuita) ed una password avente durata temporale limitata (OTP, "*one time password*"), sotto forma sia di codice numerico sia di quick response code (QR code), che il firmatario dovrà comporre utilizzando il numero di cellulare che, sulla base di quanto dichiarato dallo stesso firmatario in sede di identificazione, si trova nella sua piena ed esclusiva disponibilità,

Oppure,

- Il computer o tablet visualizza una password avente durata temporale limitata (OTP, "*one time password*") sotto forma di codice numerico. Contestualmente il sistema effettuerà una chiamata al numero di cellulare che, sulla base di quanto dichiarato dallo stesso firmatario in sede di identificazione, si trova nella piena ed esclusiva disponibilità del firmatario al fine di consentire allo stesso l'inserimento di predetto codice OTP.

Oppure,

- la Soluzione FEA trasmette all'Utente l'OTP via SMS, al numero di cellulare valorizzato in fase di enrollment, che si trova nell'esclusiva disponibilità del firmatario. Quest'ultimo dovrà quindi inserire l'OTP ricevuto nell'apposito campo dell'interfaccia web..

Le informazioni raccolte dal sistema durante i processi sopradescritti sono inserite all'interno di ogni firma in una struttura dati criptata (c.d. "blob") all'interno del documento sottoscritto collegando quindi in maniera univoca la firma, il firmatario ed il documento sottoscritto.

9.5 Possibilità di verifica che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma

Al termine della sottoscrizione, una volta esaurito il processo di cifratura di cui al precedente punto 4.4, il documento informatico è firmato o sigillato digitalmente mediante l'utilizzo di chiavi crittografiche di lunghezza non inferiore a 2048 bit, a garanzia dell'inalterabilità del documento sottoscritto.

L'operazione precedentemente descritta consente di garantire che non sia stato possibile nel tempo alterare o modificare il predetto documento informatico sottoscritto dal firmatario.

9.6 Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto

All'atto della presentazione del documento per la sottoscrizione, il firmatario può visualizzare il contenuto in tutte le sue parti sul dispositivo o sul computer. Successivamente, all'esito del processo di firma sopra descritto, il firmatario su richiesta al Soggetto Erogatore può ricevere, visualizzare e conservare il documento elettronico da lui sottoscritto che gli è stato inviato secondo il canale indicato dall'Utente firmatario nel modulo di adesione. Il documento informatico sottoscritto sarà inoltre, se richiesto dal Cliente, reso disponibile su supporto cartaceo.

9.7 Individuazione del Soggetto Erogatore della soluzione FEA

Nel modulo di adesione al servizio di FEA viene espressamente indicato, con tutti i suoi dati identificativi, chi è il soggetto che eroga la soluzione di FEA ai sensi dell'art 55, comma 2, lett. a), del DPCM.

9.8 Assenza nell'oggetto della sottoscrizione di qualunque elemento idoneo a modificarne gli atti, i fatti e i dati in esso rappresentati

I documenti prodotti dal sistema utilizzano esclusivamente formati atti a garantire l'assenza di qualunque elemento idoneo a modificare gli atti, i fatti e i dati in essi rappresentati. I documenti sono esclusivamente in formato standard ISO PDF/A (non contenente script, macro, campi da riempire od altri elementi che, dopo la generazione, potrebbero alterarne il contenuto).

9.9 Connessione univoca della firma al documento sottoscritto

I dati della firma, integrati con informazioni aggiuntive, vengono inseriti nel documento in una struttura dati (denominata "blob") che li unisce indissolubilmente all'impronta informatica (hash) del documento sottoscritto. Questa struttura è protetta con opportuna tecnica crittografica, al fine di preservare la firma da ogni possibilità di accesso ai dati, estrazione o duplicazione. L'unica chiave crittografica (chiave privata) in grado di estrarre le informazioni è in esclusivo possesso e custodita da un soggetto terzo fiduciario e potrà essere usata in sede di perizia per attestare l'autenticità del documento e della sottoscrizione. Inoltre, la soluzione appone a sigillatura dell'intero documento informatico sottoscritto con FEA una firma digitale nel formato standard PAdES, visibile e verificabile con gli strumenti informatici standard per la presentazione e lettura dei documenti (es. PDF Reader).
Nel caso di sottoscrizione mediante certificato one-shot non qualificato, la connessione univoca della firma al documento è garantita direttamente dall'apposizione di un certificato digitale sul documento informatico. Il certificato one-shot, essendo di tipo usa e getta, è utilizzato esclusivamente per la singola operazione di firma e non richiede la creazione di una struttura dati cifrata (blob).

9.10 Operazione di generazione, consegna e conservazione della chiave di criptazione

I dati utilizzati per la sottoscrizione a mezzo FEA e relativi all'identificazione certa dell'Utente Firmatario sono automaticamente cifrati all'interno del "blob" del documento informatico con una chiave di crittografia.

La predetta chiave di criptazione è generata da una terza parte fidata (es. Certificatore Accreditato o Notaio) mediante una procedura sicura ed a norma. La chiave di criptazione è depositata, custodita e conservata in forma segregata presso la predetta terza parte fidata.

Il trasferimento dei dati e la loro memorizzazione nel "blob" del documento informatico è protetto con le seguenti tecnologie crittografiche:

- crittografia simmetrica standard AES con chiave a 256 bit segreta per la protezione dei dati;
- RSA 2048 bit (o superiore) con relativa chiave privata detenuta da una terza parte per la cifratura della chiave AES;
- firma digitale di sigillatura del documento PDF in formato PAdES.

Nel caso di firma con certificato one-shot non qualificato, i dati identificativi del firmatario (nome, cognome, codice fiscale e indirizzo e-mail) sono contenuti direttamente nel certificato digitale emesso dalla Certificate Authority (CA) privata. La chiave privata associata al certificato one-shot è generata e custodita in ambiente sicuro da TeamSystem o dai fornitori ai quali eventualmente si appoggia e utilizzata esclusivamente per la singola operazione di firma.

9.11 Verifica dell'autenticità della FEA

I dati utilizzati per la sottoscrizione a mezzo FEA e relativi all'identificazione certa dell'utente firmatario sono accessibili unicamente per eventuali accertamenti nei casi previsti dalla vigente normativa, ad esempio nell'ipotesi di contestazione dell'autenticità o disconoscimento della sottoscrizione apposta sul documento, previa autorizzazione o richiesta dell'Autorità Giudiziaria.
Nel caso di firma apposta mediante certificato one-shot non qualificato, i dati identificativi del firmatario contenuti nel certificato digitale sono direttamente accessibili e verificabili con gli strumenti informatici standard per la lettura dei documenti firmati digitalmente (es. Adobe Reader), senza necessità di ricorrere a procedure di decifratura.
In tal caso, l'accesso a tali dati, incapsulati in forma criptata, sarà garantito dall'utilizzo di una solida chiave di criptazione da parte del terzo fiduciario (ad esempio il Certificatore Accreditato) che la custodisce, indispensabile per decifrare i dati della firma, ed il cui utilizzo sarà consentito esclusivamente secondo una specifica procedura di garanzia.

Il processo di decodifica avviene nel rispetto di rigorose misure di sicurezza; nel corso dell'intero processo la chiave di criptazione viene mantenuta segreta per non invalidare eventuali altri documenti con la stessa firmati.

La procedura di garanzia per l'apertura dei dati di firma incapsulati nel documento si svolgerà secondo le indicazioni della terza parte fidata. Ogni attore concorrerà alla procedura fornendo i dati di sua competenza: ad esempio il Soggetto Erogatore con il documento informatico contenente i dati del firmatario in forma cifrata e la terza parte con la chiave privata di criptazione.

Una volta decifrati i dati della firma, il perito potrà effettuare il proprio lavoro eseguendo i controlli del caso. Al termine, proprio come per una firma autografa, il perito potrà dichiarare se, a suo parere, la firma è autentica oppure no.

9.12 La sicurezza della FEA realizzata dal Soggetto Erogatore

4.12.1 FEA Grafometrica

Ogni firma del firmatario prima di essere accettata deve superare una serie di rigidi controlli di sicurezza che hanno l'obbiettivo di impedire l'uso o riuso fraudolento delle firme stesse.

Inoltre:

- ogni firma è sempre cifrata e può essere decifrata solo ricorrendo all'intervento di un terzo fiduciario designato secondo apposita procedura;
- la decifratura della firma può avvenire solo su richiesta del firmatario e delle autorità competenti;

- l'hash (trasformazione del blob in una sequenza numerica tramite un algoritmo matematico) di ogni sottoscrizione raccolta viene confrontato con l'archivio di tutti gli hash delle sottoscrizioni già registrate; in caso di due hash identici la procedura viene sospesa;
- ogni sottoscrizione raccolta vale per le specifiche condizioni e clausole mostrate sul signature pad o sul computer e per quel specifico documento informatico: ciò significa che è impossibile riutilizzare quella sottoscrizione per una diversa clausola o per la stessa clausola ma di un altro documento;
- solo dai signature pad abilitati dal Soggetto Erogatore, con apposita procedura informatica di inizializzazione, è possibile per il firmatario apporre una firma su un documento informatico; ciò significa che non è possibile utilizzare signature pad diversi da quelli del Soggetto Erogatore.

4.12.2 FEA In Mobilità o con certificato one-shot

Ogni sottoscrizione del firmatario prima di essere accettata deve superare una serie di rigidi controlli di sicurezza che hanno l'obiettivo di impedire un eventuale loro utilizzo fraudolento.

Inoltre:

- l'insieme dei dati relativi ad ogni sottoscrizione (blob) è sempre cifrato e può essere decifrato solo ricorrendo all'intervento di un terzo fiduciario designato secondo apposita procedura;
- la decifratura del blob relativo a ciascuna sottoscrizione può avvenire solo su richiesta del firmatario e delle autorità competenti;
- l'hash (trasformazione del blob in una sequenza numerica tramite un algoritmo matematico) di ogni sottoscrizione raccolta può venir confrontato con l'archivio di tutti gli hash delle sottoscrizioni già registrate; in caso di due hash identici la procedura viene sospesa;
- ogni sottoscrizione contiene un identificativo univoco della transazione utile all'eventuale recupero dei dati presenti nel sistema di Strong Authentication.

Nel caso di firma con certificato one-shot non qualificato, la sicurezza della sottoscrizione è garantita dall'emissione di un certificato digitale usa e getta associato univocamente al firmatario e alla specifica operazione di firma. Il certificato one-shot, una volta utilizzato, non è più valido per ulteriori operazioni o per attività legate al suo ciclo di vita (sospensione o revoca), impedendo qualsiasi riutilizzo fraudolento.

9.13 Certificazione ISO/IEC 27001 del produttore della tecnologia FEA

Il produttore TeamSystem S.p.A, che realizza la tecnologia software della soluzione FEA, offerta al Soggetto Erogatore mediante la Piattaforma Hub TeamSystem Digital, possiede una certificazione di conformità ISO/IEC 27001:2022 del proprio sistema di gestione per la sicurezza delle informazioni, con ambito "*design, development, installation and maintenance of informatic systems and application*".
Per quanto riguarda la soluzione di firma con certificato one-shot non qualificato, la tecnologia di emissione e gestione dei certificati è fornita da Telecom Italia Trust Technologies S.r.l., Certificate Authority che opera nel rispetto delle normative vigenti in materia di servizi fiduciari.

9.14 La descrizione della copertura assicurativa

La polizza assicurativa per la responsabilità civile, conforme a quanto previsto dall'art. 57, comma 2, del DPCM, è stipulata e gestita da TeamSystem.
Tale polizza, rilasciata da una società di assicurazione abilitata ad operare nel settore dei rischi industriali e con un massimale non inferiore a euro cinquecentomila (€ 500.000), è finalizzata a tutelare gli Utenti (firmatari della FEA) e i terzi da eventuali danni derivanti da inadeguate soluzioni tecniche adottate per l'erogazione della soluzione di FEA, coerentemente con quanto disciplinato nel contratto.

Gli estremi della polizza stipulata dal Soggetto Erogatore a tal fine sono riportati nel modulo di adesione al servizio di che ciascun Utente sottoscrive.

9.15 Modalità di richiesta assistenza e copia del modulo di adesione FEA

Il Soggetto Erogatore indica all'Utente nel modulo di adesione al servizio di FEA il canale e l'indirizzo a cui poter indirizzare tutte le comunicazioni e le richieste di assistenza inerenti la soluzione di FEA erogata, tra le quali a titolo non esaustivo la richiesta di ricevere copia, informatica o cartacea, del modulo di adesione al servizio di FEA da questi sottoscritto.

Inoltre, il Soggetto Erogatore nel modulo di adesione, compilato e sottoscritto dall'Utente, acquisisce i canali e gli indirizzi per poter successivamente consegnare all'Utente stesso i documenti informatici da lui sottoscritti e richiesti, a partire dal modulo di adesione.

9.16 La revoca dalla soluzione FEA

Le revoca potrà avvenire da parte dell'Utente firmatario in qualsiasi momento, a titolo gratuito, ed il relativo modulo di revoca va richiesto dall'Utente al Soggetto Erogatore, secondo quanto indicato nelle Condizioni generali per l'utilizzo della FEA. La revoca non ha effetto sui documenti già sottoscritti antecedentemente alla data di revoca.
Il processo di revoca dell'adesione è subordinato ai seguenti passi operativi:
- identificazione dell'Utente firmatario;
- sottoscrizione del modulo di revoca messo a disposizione che deve essere conservato almeno per venti anni;
- registrazione della revoca nell'applicativo della soluzione FEA.

Nel caso di utilizzo della soluzione di FEA con certificato one-shot non qualificato, si precisa che il certificato digitale, essendo di tipo one-shot (usa e getta), non è soggetto a revoca o sospensione in quanto viene utilizzato esclusivamente per una singola operazione di firma e non è più valido successivamente. La gestione del ciclo di vita dei certificati one-shot è a carico della Certificate Authority emittente.

9.17 Requisiti della soluzione FEA ai sensi dell'Art. 56 del DPCM

L'articolo 56 del DPCM 22 febbraio 2013 definisce le caratteristiche obbligatorie delle soluzioni di firma elettronica avanzata. La tabella seguente correla ciascun requisito normativo alle specifiche caratteristiche tecniche implementate nella presente soluzione FEA.

Requisito ex Art. 56 DPCM 22/02/2013	Caratteristica della soluzione FEA adottata

È connessa unicamente al Firmatario	La procedura di firma può essere attivata esclusivamente dal firmatario tramite inserimento dell'OTP ricevuta sul numero di cellulare certificato dal Soggetto Erogatore e associato univocamente al firmatario in fase di identificazione, oppure tramite apposizione della firma autografa su signature pad sotto il diretto controllo del firmatario. Nel caso di certificato one-shot, la chiave privata è invocabile esclusivamente a seguito del buon esito dell'autenticazione.
È idonea a identificare il Firmatario	I dati identificativi del firmatario, acquisiti dall'Erogatore in fase di riconoscimento, sono associati alla firma. Nel caso di certificato one-shot, tali dati sono direttamente contenuti nel certificato digitale emesso a nome del firmatario dalla CA privata.
È creata mediante dati per la generazione della firma che il Firmatario può utilizzare sotto il proprio esclusivo controllo	I dati per la generazione della firma includono: l'OTP trasmessa al firmatario via SMS o chiamata, e – nel caso di certificato one-shot – la chiave privata del certificato, invocabile solo dopo autenticazione riuscita. I dati grafometrici, per la modalità FEA Grafometrica, sono acquisiti in esclusiva disponibilità del firmatario.
È collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati	I meccanismi crittografici di firma e sigillatura assicurano l'integrità del documento sottoscritto e rendono rilevabile qualsiasi alterazione successiva all'apposizione della firma.
Possibilità per il Firmatario di ottenere evidenza di quanto sottoscritto	I documenti sottoscritti sono messi a disposizione del firmatario dal Soggetto Erogatore, attraverso il canale di comunicazione indicato nel modulo di adesione. Il firmatario può richiederne copia in qualsiasi momento.
Individuazione del soggetto di cui all'art. 55, comma 2, lett. a) DPCM (soggetto erogatore)	I riferimenti identificativi del Soggetto Erogatore sono indicati nel presente Manuale Tecnico e nel modulo di adesione messo a disposizione del firmatario prima dell'adesione al servizio.
Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati	I documenti oggetto di sottoscrizione sono prodotti in formato PDF/A, standard ISO privo di script, macro, campi compilabili o altri elementi che potrebbero modificarne il contenuto dopo la generazione, conformemente al CAD e al DPCM 13 novembre 2014 [4].
È connessa univocamente al documento sottoscritto	L'autenticazione del firmatario e la successiva apposizione della firma nei campi del documento rappresentano operazioni univocamente associate alla specifica transazione di firma, non replicabili su documenti diversi.

9.18 Conservazione a norma dei documenti sottoscritti

Al completamento del processo di sottoscrizione, il documento informatico firmato, unitamente alle evidenze acquisite durante le fasi di adesione e di firma, deve essere inviato in conservazione a norma da parte e cura del Soggetto Erogatore. Il processo di conservazione deve essere condotto in conformità al DPCM 3 dicembre 2013 [5] e alle disposizioni del Codice dell'Amministrazione Digitale, al fine di garantire nel tempo l'integrità, l'autenticità, la leggibilità e la reperibilità dei documenti e delle relative evidenze.

Il Soggetto Erogatore è responsabile dell'invio in conservazione e può avvalersi di un conservatore accreditato o di un sistema di conservazione conforme ai requisiti di legge. Le evidenze conservate comprendono, a titolo esemplificativo e non esaustivo: il documento informatico sottoscritto, il

modulo di adesione firmato, la copia del documento di riconoscimento del firmatario e i metadati relativi alla transazione di firma.

Torna al sommario