

# SCHEDA TECNICA ILLUSTRATIVA SULLA FIRMA ELETTRONICA AVANZATA

Il presente documento (di seguito “Nota Informativa”) è predisposto da Iren Mercato SpA (di seguito la “Società”) ai sensi dell’articolo 57, commi 1 lett. e), del DPCM 22/02/2013, contenente le regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali (di seguito “Decreto Regole Tecniche”), pubblicato nella Gazzetta Ufficiale n. 117 del 21/05/2013, attuativo del Codice dell’Amministrazione Digitale (Decreto Legislativo n. 82 del 07/03/2005, di seguito “CAD”).

## 1. INFORMAZIONI GENERALI

### 1.1. La firma elettronica avanzata in modalità remota

Nell’ambito delle iniziative volte ad innovare e a migliorare l’efficienza dei propri processi, la Società ha introdotto una nuova modalità di firma dei documenti basata su una soluzione informatica che consente di sottoscrivere i documenti in formato elettronico, con l’obiettivo di ridurre e, ove possibile, eliminare nel corso del tempo l’uso della carta.

La sottoscrizione dei predetti documenti tramite una firma elettronica avanzata (d’ora in avanti “FEA”) in modalità remota avviene mediante un processo informatico attraverso il quale il firmatario viene identificato dal servizio e autorizza l’apposizione della firma tramite un meccanismo di sicurezza.

Il documento recante la sottoscrizione del firmatario viene memorizzato e sigillato tramite apposizione della firma digitale della Società, che rende immodificabile il documento così sottoscritto.

Conclusa l’operazione di sottoscrizione, viene avviato il processo di conservazione del documento informatico sottoscritto, conformemente alla normativa vigente e viene avviato un processo di notarizzazione su blockchain che consente ottenere tutta una serie di funzionalità per la verifica immediata e trasparente di tutte le caratteristiche del processo di firma incrementandone i requisiti di sicurezza e accertamento.

La firma e l’intero servizio di firma elettronica sono resi disponibili al firmatario dalla Società, ai sensi dell’art. 55, comma 2, lett. a) del Decreto Regole Tecniche.

Per l’erogazione del codesto servizio, la Società si è rivolta ad una primaria società informatica che - ai sensi dell’art. 55, comma 2, lett. b) del Decreto Regole Tecniche - realizza soluzioni di firma elettronica e il servizio di conservazione è affidato ad un ente avente qualifica di Certification Authority ai sensi della normativa vigente.

### 1.2. I documenti che possono essere sottoscritti con la Firma Elettronica

La Firma Elettronica consentirà al cliente di sottoscrivere tutti i documenti per i quali la Società avrà reso, nel corso del tempo, disponibile tale servizio.

### 1.3. Il processo di sottoscrizione

Il servizio di Firma Elettronica consente al cliente di:

- visualizzare e leggere il documento sullo schermo del proprio dispositivo;
- sottoscrivere il documento direttamente sul dispositivo in modalità elettronica.

Al termine dell’operazione di sottoscrizione, il documento informatico assume caratteristiche tecniche che ne garantiscono l’integrità e l’immodificabilità.

### 1.4. La consegna del documento informatico sottoscritto

Il documento informatico è consegnato al cliente che lo ha sottoscritto rendendolo accessibile tramite mail. Il cliente firmatario al termine del processo di sottoscrizione riceverà una mail all’indirizzo di posta elettronica comunicato con un link per effettuare il download della sua copia firmata. Diversamente potrà richiedere la stampa del documento. Qualora il Cliente nel corso del tempo vari l’indirizzo di posta elettronica, dovrà comunicare il nuovo indirizzo alla Società.

### 1.5. La conservazione a norma dei documenti informatici sottoscritti dal contraente

I documenti informatici ai quali è stata apposta la Firma Elettronica vengono inviati ad un soggetto terzo (abilitato a svolgere il servizio di conservazione dei documenti informatici) per la conservazione conforme alla normativa vigente, disciplinata nel CAD e nelle norme attuative (in particolare, il Decreto del Presidente del Consiglio dei Ministri del 3/12/2013, pubblicato nella Gazzetta Ufficiale n. 59 del 12/03/2014).

La conservazione ha lo scopo di conferire al documento informatico le caratteristiche di immodificabilità, autenticità, integrità affidabilità, leggibilità e reperibilità, tramite la memorizzazione dei documenti informatici su di un idoneo supporto informatico che ne permette la conservazione per la durata prevista dalla legge. Una volta concluso il processo di sottoscrizione dei documenti, il documento informatico è inviato dal fornitore del servizio di firma al conservatore accreditato. Periodiche verifiche sull’integrità e la leggibilità dei documenti sono svolte sul sistema di conservazione al fine di garantire un alto livello di affidabilità e di qualità del servizio.

## 2. LA DICHIARAZIONE DI ACCETTAZIONE DELL’UTILIZZO DELLA FEA REMOTA

L’utilizzo della FEA Remota può avvenire solo successivamente all’esplicita accettazione, da parte del firmatario, di avvalersi di tale modalità di firma.

Tale accettazione è espressa in una specifica dichiarazione denominata “modulo di adesione FEA” che la Società sottopone al firmatario unitamente alla presente Nota informativa e all’informativa sul trattamento dei dati personali che il firmatario accetta e sottoscrive. Al momento della sua sottoscrizione, copia di tale modulo di adesione è rilasciata al firmatario, rendendola disponibile, in formato pdf, come descritto al punto 1.4.

Il modulo di adesione contenente la dichiarazione di accettazione delle condizioni del servizio di Firma Elettronica Avanzata (FEA) e la copia del documento di riconoscimento con cui è avvenuta l'identificazione del firmatario saranno conservati dalla Società per almeno venti anni.

La mancata accettazione del servizio di Firma Elettronica rende impossibile firmare i documenti in modalità elettronica; rimane possibile firmare in modalità tradizionale con firma autografa.

In qualunque momento l'accettazione potrà essere liberamente revocata dal cliente, che potrà quindi tornare a sottoscrivere eventuali successivi documenti con la tradizionale firma autografa apposta sui documenti cartacei.

### **3. LE CARATTERISTICHE DEL SISTEMA DI FIRMA ELETTRONICA REMOTA**

#### **3.1. Caratteristiche del sistema che garantiscono l'identificazione del firmatario**

Il firmatario viene identificato dalla Società tramite un processo Video Selfie che richiede tra l'altro anche la cattura della copia del documento d'identità (carta di identità, patente, passaporto, ...).

Alternativamente il firmatario viene identificato tramite una autenticazione SPID di Livello 2; l'accesso tramite credenziali SPID garantisce l'identificazione effettuata in origine dall'Identity Provider SPID.

#### **3.2. Caratteristiche del sistema che garantiscono la connessione univoca della firma al firmatario**

##### **3.2.1. FEA OTP SMS**

La modalità di FEA Remota con OTP SMS è basata sull'utilizzo del telefono cellulare del firmatario. Il firmatario, dopo aver preso visione della documentazione da sottoscrivere, ivi incluso il modulo di adesione al servizio FEA, esprime manualmente la propria volontà di sottoscrizione attraverso un processo di "Point and Click" e una successiva transazione di conferma effettuata tramite OTP SMS. Ciò significa che l'utente firmatario riceve un OTP (One-Time-Password) di firma via SMS al numero di cellulare che ha dichiarato essere sotto il suo controllo esclusivo ed inserisce l'OTP sullo schermo dal quale sta visualizzando il documento da firmare. Le informazioni raccolte dal sistema durante la transazione di firma sono inserite all'interno di ogni firma nel cosiddetto "blob di firma" e collegano in maniera univoca quella firma al firmatario, e/o tali informazioni vengono notarizzate in Blockchain. Il sistema certifica che l'utente firmatario abbia inserito l'OTP relativo a quella transazione (e relativo a quel documento).

##### **3.2.2. FEA con SPID**

La modalità di FEA Remota con SPID è basata sull'utilizzo delle proprie credenziali SPID e della propria identità certificata e garantita dall'Identity Provider. L'utente firmatario utilizza perciò le proprie credenziali SPID per firmare la documentazione proposta; il sistema certifica e tiene traccia di tutti i passaggi che l'utente ha seguito per effettuare la firma, compreso il nome dell'Identity Provider e la relativa risposta di autenticazione che l'Identity Provider stesso. Le informazioni raccolte dal sistema durante la transazione di firma sono inserite all'interno di ogni firma nel cosiddetto "blob di firma" e collegano in maniera univoca quella firma al firmatario, e/o tali informazioni vengono notarizzate in Blockchain.

#### **3.3. Caratteristiche del sistema che garantiscono il controllo esclusivo del firmatario sul sistema di generazione della firma**

In fase di adesione al servizio FEA l'utente firmatario fornisce 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 e controllo esclusivo.

#### **3.4. Caratteristiche del sistema che garantiscono di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma**

##### **3.4.1. FEA OTP SMS**

Al termine della sottoscrizione il documento informatico è firmato digitalmente con certificato qualificato emesso da una Certification Authority riconosciuta. La tecnologia di firma digitale include l'impronta informatica (HASH) del contenuto soggetto a sottoscrizione. Il controllo della corrispondenza tra un'impronta ricalcolata e quella "sigillata" all'interno delle firme permette di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma. Questo consente di rilevare ogni possibile alterazione o modifica effettuata al documento. Inoltre, l'HASH del documento firmato e sigillato viene notarizzato su Blockchain, il che ne garantisce ulteriormente l'immodificabilità.

##### **3.4.2. FEA con SPID**

Come per la FEA con SMS, al termine della sottoscrizione il documento informatico è firmato digitalmente con certificato qualificato emesso da una Certification Authority riconosciuta. La tecnologia di firma digitale include l'impronta informatica (HASH) del contenuto soggetto a sottoscrizione. Il controllo della corrispondenza tra un'impronta ricalcolata e quella "sigillata" all'interno delle firme permette di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma. Questo consente di rilevare ogni possibile alterazione o modifica effettuata al documento. Inoltre, l'HASH del documento firmato e sigillato viene notarizzato su Blockchain, il che ne garantisce ulteriormente l'immodificabilità.

#### **3.5. Caratteristiche del sistema che garantiscono la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto**

##### **3.5.1. FEA OTP SMS**

All'atto della presentazione del documento per la firma, il firmatario può visualizzare sul video il contenuto in tutte le sue parti, con apposite funzioni di posizionamento. Successivamente, il Cliente firmatario potrà visualizzare il documento elettronico firmato scaricandolo tramite un link che verrà inviato all'indirizzo di posta personale che il Cliente ha dichiarato in fase di adesione, oppure ricevendolo direttamente come allegato alla suddetta e-mail.

##### **3.5.2. FEA con SPID**

Come per la FEA OTP SMS, all'atto della presentazione del documento per la firma, il firmatario può visualizzare sul video il contenuto in tutte le sue parti, con apposite funzioni di posizionamento. Successivamente, il Cliente firmatario potrà visualizzare il documento elettronico firmato scaricandolo tramite un link che verrà inviato all'indirizzo di posta personale che il Cliente ha dichiarato in fase di adesione, oppure ricevendolo direttamente come allegato alla suddetta e-mail.

### 3.6. Caratteristiche del sistema che garantiscono l'individuazione del soggetto erogatore della soluzione Firma Elettronica

Il certificato di firma digitale o sigillo individua il soggetto erogatore del servizio ed è emesso da una Certification Authority. In questo caso ogni contratto con la clientela, dopo la raccolta delle firme, viene sigillato tramite apposizione della firma digitale della Società rilasciata dalla Certification Authority.

### 3.7. Caratteristiche del sistema che garantiscono l'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, nell'oggetto della sottoscrizione, di qualunque elemento idoneo a modificare gli atti, i fatti e i dati in essi rappresentati. Ad esempio, attualmente, i documenti sono esclusivamente in formato standard ISO PDF/A.

### 3.8. Caratteristiche del sistema che garantiscono la connessione univoca della firma al documento sottoscritto

#### 3.8.1. FEA OTP SMS

I dati della firma vengono inseriti nel documento in una struttura, detta "blob di firma", che li unisce indissolubilmente all'impronta informatica del documento sottoscritto. Questa struttura è protetta con opportuna tecnica crittografica, al fine di preservare la firma da ogni possibilità di estrazione o duplicazione. La chiave crittografica in grado di estrarre le informazioni contenute nel blob è in esclusivo possesso di una terza parte fidata dotata di idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave. Questa chiave potrà essere usata in sede di perizia espressamente nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma e a seguito di richiesta dell'autorità giudiziaria per attestare l'autenticità del documento e della sottoscrizione.

Inoltre, il sistema appone a sigillatura dell'intero contratto una "firma digitale" in formato standard PADES. A differenza del "blob di firma" questa tipologia di firma è visibile e verificabile con gli strumenti informatici standard per la presentazione e lettura dei documenti (es. PDF Reader).

Nel caso di notarizzazione su Blockchain la verifica è demandata al confronto tra l'HASH del documento in possesso all'utente e l'HASH notarizzato; l'utente ha perciò la possibilità di effettuare la verifica in autonomia.

#### 3.8.2. FEA con SPID

I dati della firma vengono inseriti nel documento in una struttura, detta "blob di firma", che li unisce indissolubilmente all'impronta informatica del documento sottoscritto. Questa struttura è protetta con opportuna tecnica crittografica, al fine di preservare la firma da ogni possibilità di estrazione o duplicazione. La chiave crittografica in grado di estrarre le informazioni contenute nel blob è in esclusivo possesso di una terza parte fidata dotata di idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave. Questa chiave potrà essere usata in sede di perizia espressamente nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma e a seguito di richiesta dell'autorità giudiziaria per attestare l'autenticità del documento e della sottoscrizione.

Inoltre, il sistema appone a sigillatura dell'intero contratto una "firma digitale" in formato standard PADES. A differenza del "blob di firma" questa tipologia di firma è visibile e verificabile con gli strumenti informatici standard per la presentazione e lettura dei documenti (es. PDF Reader).

Nel caso di notarizzazione su Blockchain la verifica è demandata al confronto tra l'HASH del documento in possesso all'utente e l'HASH notarizzato; l'utente ha perciò la possibilità di effettuare la verifica in autonomia.

## 4. REVOCA DEL CONSENSO ALL'UTILIZZO DELLA SOLUZIONE DI FIRMA ELETTRONICA AVANZATA

Gli utenti che hanno aderito al servizio FEA possono richiedere, in qualsiasi momento tramite apposito modulo/scrivendo una mail all'indirizzo clienti.nuoviprodotti@irenmercato.it, la revoca all'adesione tornando quindi ad operare con la tradizionale firma autografa su documentazione cartacea.

## 5. INFORMAZIONI RIGUARDANTI LA COPERTURA ASSICURATIVA

In conformità alla normativa vigente, al fine di proteggere i titolari della firma elettronica avanzata e i terzi da eventuali danni cagionati da inadeguate soluzioni tecniche adottate, la soluzione di Firma Elettronica Avanzata adottata dalla Società è coperta da polizza assicurativa rilasciata da una primaria compagnia di assicurazione, abilitata ad esercitare nel campo dei rischi industriali e la copertura assicurativa rispetta i massimali imposti dalla normativa.