SCHEDA ILLUSTRATIVA DELLE CARATTERISTICHE TECNICHE DEL SISTEMA DI FIRMA ELETTRONICA AVANZATA (FEA) E DELLE TECNOLOGIE UTILIZZATE

Ai sensi degli artt. 56 e 57, lett. e) ed f), del Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 ("Regole Tecniche")

Il servizio FEA prevede l'attivazione e la configurazione del DTM Intesa per abilitare il processo digitale di firma dei contratti.

1. La descrizione delle caratteristiche del sistema che garantiscono l'identificazione del firmatario
   Il censimento e l'identificazione *de visu* del cliente finale avviene da parte del personale dipendente di Assicura Agenzia, nonché degli intermediari assicurativi con cui collabora (con tale locuzione, anche nel prosieguo del testo, devono intendersi i dipendenti dei soggetti iscritti al RUI con cui Assicura Agenzia collabora in forza di specifici accordi di collaborazione).
   L'identificazione del firmatario avviene in modo certo, richiedendo il documento d'identità di quest'ultimo in corso di validità ed acquisendone copia in fase di adesione al Servizio FEA.
   La copia del documento d'identità ed il modulo di adesione al Servizio FEA sottoscritto dal firmatario sono conservati per 20 anni, in conformità alla normativa vigente.
2. La descrizione delle caratteristiche del sistema che garantiscono la connessione univoca della firma al firmatario
   L'univocità della connessione della firma al firmatario – già identificato previa presentazione di un documento di identità in corso di validità – viene garantita mediante l'invio del documento oggetto di firma all'indirizzo e-mail di quest'ultimo, nonché dall'invio di una OTP (*One Time Password*) al cellulare dello stesso, di cui dichiara di avere – in quel momento e per tutto l'arco di tempo del processo di sottoscrizione – piena ed esclusiva disponibilità.
   L'OTP ricevuta dal cliente viene, quindi, digitata manualmente all'interno dello specifico spazio dedicato per la sottoscrizione del documento. Le informazioni raccolte dal sistema durante la transazione sono inserite all'interno di ogni firma e collegano in maniera univoca quella firma al firmatario.
   Il sistema certifica che il numero dichiarato come proprio dell'utente è stato destinatario dell'SMS contenente la OTP relativa a quella transazione e a quello specifico documento.
3. La descrizione delle caratteristiche del sistema che garantiscono il controllo esclusivo del firmatario sul sistema di generazione della firma
   Durante la fase di firma, il sistema è nella piena ed esclusiva disponibilità, nonché sotto il controllo esclusivo del firmatario, il quale, prima di apporre la propria firma, può consultare sul dispositivo dell'intermediario il documento informatico per controllarne direttamente i contenuti: tale documento ripropone integralmente le caratteristiche delle corrispondenti versioni documentali cartacee.
   Il firmatario ha la possibilità di verificare personalmente i propri dati ed ogni dettaglio contrattuali, procedendo in autonomia alla lettura delle clausole ed alla selezione dei relativi campi di firma sui quali è chiamato ad esprimere manualmente (processo

di *point and click*) la propria volontà di sottoscrizione. Durante la sottoscrizione il cliente può effettuare l'annullamento dell'operazione di firma e ripetere la sottoscrizione.
Conclusa tale fase, l'utente visualizza una schermata recante il nome del firmatario, il suo numero di cellulare, il riepilogo di tutti i campi per la sottoscrizione da lui selezionati, nonché la richiesta di confermare quanto indicato.
Dopo la conferma, al numero di cellulare indicato – nella sua piena ed esclusiva disponibilità – riceverà dalla *Certification Authority* un SMS contenente una password avente una durata temporale limitata (OTP) sotto forma di codice numerico che il firmatario deve inserire nella piattaforma per procedere alla apposizione della firma elettronica.
La *Certification Authority,* riconosciute e validate le informazioni (numero di cellulare e OTP), provvede ad informare il sistema dell'avvenuta manifestazione di volontà di sottoscrizione da parte del firmatario (processo di *strong authentication* e sottoscrizione). Le operazioni sopra descritte e l'esito della transazione con la *Certification Authority* sono quindi inserite all'interno del documento stesso e automaticamente criptate.

4. La descrizione delle caratteristiche del sistema che garantiscono di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma
   L'integrità del documento informativo sottoscritto con processo FEA è attestata attraverso l'impiego di tecnologie crittografiche e di algoritmi di hash (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), nonché da una marcatura temporale che attesta in modo preciso la data e l'ora in cui la firma è stata apposta.
   Il cliente ha sempre la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma: presso l'Agenzia per l'Italia Digitale (AgID), all'indirizzo http://www.agid.gov.it/identita-digitali/firme-elettroniche/software-verifica sono disponibili software gratuiti per effettuare tale verifica.
5. La descrizione delle caratteristiche del sistema che garantiscono la 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, con apposite funzioni di posizionamento.
   Successivamente, all'esito del processo di firma sopra descritto, il firmatario può visualizzare e conservare il documento elettronico da lui sottoscritto, che è inviato alla casella di posta elettronica comunicata dallo stesso.
   Il documento informatico sottoscritto – se richiesto dal cliente – viene inoltre reso disponibile contestualmente su supporto cartaceo.
6. La descrizione delle caratteristiche del sistema che garantiscono l'individuazione del soggetto erogatore della soluzione FEA
   Il servizio FEA viene fornito da Assicura Agenzia in collaborazione con gli intermediari assicurativi con cui la medesima collabora, i quali – ai sensi dell'art. 55, comma 2, lett. a) delle Regole Tecniche del Dpcm 22 febbraio 2013 – erogano il suddetto servizio nell'ambito dei rapporti intrattenuti con la clientela.

7. La descrizione delle caratteristiche del sistema che garantiscono l'assenza nell'oggetto della sottoscrizione di qualunque elemento idoneo a modificare 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 esso rappresentati.

   L'utilizzo di documenti PDF/A consente di accertare l'assenza di codici eseguibili o macroistruzioni all'interno dei documenti sottoscritti. In tal modo è possibile garantire che il documento prodotto sia in un formato tale da impedire l'inserimento all'interno dello stesso di programmi o istruzioni potenzialmente in grado di modificare gli atti, i fatti o i dati rappresentati nel documento medesimo.

   I documenti così generati vengono infine archiviati da Allitude (Società del Gruppo Bancario Cooperativo Cassa Centrale Banca specializzata in servizi di outsourcing informatico) secondo le norme di conservazione dei documenti previsti all'interno del Codice dell'Amministrazione Digitale (CAD), nonché in base alle Regole Tecniche di cui al Dpcm 22 febbraio 2013.
8. La descrizione delle caratteristiche del sistema che garantiscono la connessione univoca della firma al documento sottoscritto

   I dati della firma, integrati con informazioni aggiuntive, vengono inseriti nel documento in una struttura dati che li unisce indissolubilmente all'impronta informatica del documento sottoscritto generata con la funzione di hash. Questa struttura è poi protetta con opportuna tecnica crittografica, al fine di preservare la firma da ogni possibile estrazione o duplicazione.
9. La descrizione delle caratteristiche delle tecnologie utilizzate nel Servizio di firma elettronica avanzata

   Il trasferimento dei dati e la loro memorizzazione sono protetti con le seguenti tecnologie crittografiche:
   a. Algoritmo hash: SHA256
   b. Algoritmo di firma: RSA con PKCS#1 v.1.5
   c. I dati inviati verso i server Docusign sono cifrati con chiave simmetrica AES 256

L'intermediario assicurativo con cui collabora Assicura Agenzia – come previsto dall'art. 57, comma 1, lett. c) del DPCM 22 febbraio 2013 – si impegna a fornire gratuitamente una copia del Modulo di adesione sottoscritto, contenente la dichiarazione di accettazione delle condizioni del Servizio FEA, nonché copia del documento di riconoscimento fornito dal cliente per la sua identificazione, qualora quest'ultimo ne faccia ne faccia richiesta mediante invio di una e-mail all'indirizzo che l'intermediario gli fornirà.