Scheda tecnica Illustrativa

CARATTERISTICHE TECNOLOGICHE DEL SISTEMA PER L'USO DELLA FIRMA ELETTRONICA AVANZATA

ai sensi dell´art. 57, lett. e) delle 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 (Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013, il "DPCM"), attuative del Codice dell´Amministrazione Digitale (decreto legislativo 07.03.2005, n. 82, e successive modificazioni).

1. **La descrizione delle caratteristiche del sistema che garantiscono l´identificazione del firmatario.**

   I soggetti erogatori del servizio di AliasLab S.p.A. identificano in modo certo il firmatario richiedendo il relativo documento d´identità (in corso di validità), di cui acquisiscono copia in fase di adesione al servizio FEA AliasLab S.p.A.. Copia del documento d´identità ed il modulo di adesione al servizio sottoscritto dal firmatario sono conservati per 20 anni.

2. **La descrizione delle caratteristiche del sistema che garantiscono la connessione univoca della firma al firmatario.**

   a. **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 di AliasLab S.p.A. e/o altro strumento informativo equivalente (ogni Signature PAD consegnato agli erogatori del servizio è censito in un database centralizzato ed il relativo, corretto funzionamento viene verificato in remoto). 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´intermediario assicurativo, 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.

   b. **FEA non Grafometrica (FEA in Mobilità)**

   L´univocità della connessione della firma al firmatario, presupposto obbligatorio per la sottoscrizione del documento informatico, viene garantita dalla sottoscrizione effettuata davanti all´intermediario assicurativo e previo riconoscimento del firmatario mediante documento d´identità in corso di validità, nonchè dall´utilizzo da parte di quest´ultimo 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.

3. **La descrizione delle caratteristiche del sistema che garantiscono il controllo esclusivo del firmatario sul sistema di generazione della firma.**

   a. **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 11.1.

Lo schermo del dispositivo di firma (Signature PAD di AliasLab S.p.A. e/o altro strumento informatico equivalente) mostra il dettaglio della clausola oggetto della firma consentendo al firmatario di verificare personalmente i propri dati ed ogni dettaglio contrattuale. 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 SignaturePAD. Apposite funzioni consentono al firmatario di confermare o cancellare la firma in caso di errori. Il processo di firma avviene in modo automatico sulla base del programma installato sul Signature PAD utilizzato dal firmatario. 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.

   b. **FEA non 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 11.2. Il soggetto erogatore consegna il tablet al firmatario che ne entra nella piena ed esclusiva disponibilità. Il firmatario, il quale ha la possibilità di verificare personalmente su tale tablet i propri dati ed ogni dettaglio contrattuale, 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. Conclusa tale fase, il tablet 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, nonchè la richiesta di confermare quanto indicato. Dopo la conferma, il 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, si trova nella sua piena ed esclusiva disponibilità. 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 in una struttura dati ("blob") 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.**
   Al termine della sottoscrizione, una volta esaurito il processo di cifratura di cui al precedente punto 3, il documento informatico è firmato digitalmente con il certificato qualificato di AliasLab S.p.A. 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 predetto documento informatico sottoscritto dal firmatario.

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 (per motivi di sicurezza senza il vettore grafometrico), che è inviato alla casella di posta elettronica comunicata dal medesimo firmatario. Il documento informatico sottoscritto sarà inoltre, se richiesto dal Cliente, reso disponibile contestualmente su supporto cartaceo.

6. **La descrizione delle caratteristiche del sistema che garantiscono l´individuazione del soggetto erogatore della soluzione FEA.**
   Nelle condizioni generali del servizio viene espressamente indicato che AliasLab S.p.A. è il soggetto che eroga la soluzione di FEA ai sensi dell´art 55, comma 2, lett. a), del DPCM.

7. **La descrizione delle 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. 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).

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 ("blob") 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. L´unica chiave crittografica in grado di estrarre le informazioni è in esclusivo possesso di pubblico ufficiale (Studio Notarile) appositamente designato da AliasLab S.p.A., e potrà essere usata in sede di perizia per attestare l´autenticità del documento e della sottoscrizione.

Inoltre il sistema appone a sigillatura dell´intero contratto e/o altro documento oggetto di sottoscrizione una "firma digitale" in formato standard SIGNATURE PADES. Queste firme tecniche sono visibili e verificabili con gli strumenti informatici standard per la presentazione e lettura dei documenti (es. PDF Reader).

9. **Descrizione delle caratteristiche delle tecnologie utilizzate nel servizio di firma elettronica avanzata.**

   Il trasferimento dei dati e la loro memorizzazione nel "blob" 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 con chiave privata detenuta da una terza parte per la cifratura della chiave AES;
   - firma tecnica del documento PDFcon firma PADES.

10. **La descrizione delle modalità attraverso cui i clienti possono richiedere copia del modulo di adesione, da questi sottoscritto, al servizio di firma elettronica avanzata.**
    I Clienti, salva loro diversa indicazione, riceveranno in posta elettronica (o PEC), all´indirizzo dagli stessi fornito, copia della documentazione sottoscritta: modulo di adesione e documenti sottoscritti con la FEA. Se richiesto, il Cliente potrà ricevere copia stampata del contratto e/o altro documento sottoscritto e del modulo di adesione al Servizio FEA AliasLab S.p.A..

11. **La sicurezza della FEA realizzata da AliasLab S.p.A.**

    11.1 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 epuò essere decifrata solo ricorrendo all´intervento di un notaio designato secondo apposite 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 solo per la specifica clausola mostrata sul Signature PAD e per quello specifico documento: 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 da AliasLab S.p.A., con apposita procedura informatica di inizializzazione, è possibile per il firmatario apporre una firma su un contratto e/o altro documento; ciò significa che non è possibile utilizzare Signature PAD diversi da quelli certificati da AliasLab S.p.A.;
- i Signature PAD AliasLab S.p.A. sono riconoscibili a vista dal firmatario in quanto marcati col logo ALIASLAB S.P.A..

11.2. FEA non Grafometrica

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:

- ogni sottoscrizione è sempre cifrata e può essere decifrata solo ricorrendo all´intervento del notaio designato, secondo apposita procedura;
- la decifratura della sottoscrizionepuò avvenire solo su richiesta delfirmatario 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 contiene un identificativo della transazione rilasciato dalla Certification Authority che ne attesta la autenticità.

12. La descrizione della copertura assicurativa che AliasLab S.p.A. è tenuta a stipulare per la responsabilità civile da danno a terzi per un ammontare non inferiore a euro cinquecentomila.

AliasLab S.p.A., conformemente alla normativa vigente, ha stipulato polizza assicurativa di responsabilità civile N. 1/2374/65/101699109, avente massimale di euro 500.000,00, al fine di proteggere i titolari della firma elettronica avanzata e i terzi da eventuali danni cagionati da inadeguate soluzioni tecniche.

13. Il sistema di FEA di AliasLab S.p.A. ha conseguito la certificazione ISO27001 rilasciata dall´ente di certificazione internazionale DNV GL Business Assurance Italia S.r.l.

AliasLab S.p.A. ha ottenuto la certificazione ISO/IEC 27001 per l´analisi, progettazione, sviluppo, manutenzione ed erogazione del servizio di Firma Elettronica Avanzata Signature PAD ai sensi dell´art. 59, comma 1, delle Regole Tecniche. Il conseguimento, da parte di una terza parte indipendente (a ciò normativamente autorizzata), di questa certificazione del proprio sistema di gestione per la sicurezza delle informazioni a supporto della soluzione di firma elettronica avanzata proposta, da rinnovare ogni anno, è una ulteriore tutela verso il Cliente dell´adeguatezza del sistema FEA realizzato da AliasLab S.p.A..

Riepilogo delle principali caratteristiche della FEA realizzata ed erogata da AliasLab S.p.A..

a) **Identificazione del firmatario.** Il firmatario viene riconosciuto dall´intermediario assicurativo attraverso un valido documento di identità acquisito con il modulo di adesione al servizio e conservato a norma di legge.
b) **Connessione univoca della firma al firmatario.** Nel caso di utilizzo della FEA Grafometrica i dati grafometrici rilevati dal Signature PAD al momento dell´apposizione della firma con la penna elettronica sono univocamente riconducibili solo al firmatario e legati in modo indissolubile al documento informatico da lui sottoscritto, mentre nel caso di utilizzo della FEA non Grafometrica il firmatario utilizza un numero di cellulare riferito ad una SIM card di cui ha dichiarato di avere, in quel momento, piena ed esclusiva disponibilità.
c) **Controllo esclusivo del firmatario del sistema di generazione della firma, inclusi i dati biometrici.** Durante la fase della sottoscrizione il firmatario è l´unico che ha accesso e disponibilità della postazione (sia esso il Signature PAD o il Tablet) e da quel momento in poi la sua firma è cifrata e sigillata con il documento sottoscritto (nessuno può sostituire la firma né variare il contenuto del documento senza evidenza dialterazione).
d) **Possibilità di verifica che il documento informatico sottoscritto non abbia subito modifiche dopo la firma.** Questo è garantito dal processo di generazione del documento in formato PDF/A, di cifratura del vettore grafometrico e dalla firma digitale di [AliasLab S.p.A.] a chiusura del documento.
e) **Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto.** AliasLab S.p.A. invia sempre il documento informatico sottoscritto relativo al contratto e/o altro documento al Cliente via mail alla casella da lui indicata e se il Cliente lo richiede è possibile effettuare una stampa al momento della sottoscrizione.
f) **Individuazione di AliasLab S.p.A.** Nelle condizioni generali di servizio di cui il Cliente ha preso visione e che ha accettato, viene espressamente indicato che AliasLab S.p.A. è il soggetto che eroga la soluzione di FEA.
g) **Assenza di elementi nell´oggetto della sottoscrizione atti a modificarne gli atti, fatti o dati rappresentati.** Il documento d´origine è un PDF/A, quindi non auto modificabile.
h) **Connessione Univoca della firma al documento sottoscritto.** Il processo realizzato da AliasLab S.p.A. garantisce che le firme apposte dal firmatario valgano solo per la specifica clausola e per lo specifico documento in visone al firmatario. Il PDF risultante è immediatamente sigillato con la firma digitale di AliasLab S.p.A. Un eventuale documento non completato con tutte le firme e non sigillato entro un tempo stabilito verrà automaticamente annullato.
i) Signature PAD e/o altro strumento informatico equivalente su cui si appone la firma sono registrati, censiti e controllati da AliasLab S.p.A.
j) **Certificazione ISO27001** conseguita da AliasLab S.p.A. per il servizio FEA

Per ulteriori approfondimenti tecnici rifarsi alla documentazione analitica pubblicata sulla specifica sezione del sito www.aliaslab.net dedicata alla FEA.