

## Scheda tecnica illustrativa Firma Elettronica Avanzata OTP

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

La presente scheda tecnica illustra le caratteristiche della soluzione di Firma Elettronica Avanzata (FEA) per utilizzo in modalità remota erogata da Agos Ducato S.p.A. con sede legale in Milano, Viale Fulvio Testi n. 280, Codice Fiscale 08570720154 e P.IVA 08570720154 (di seguito, “**Soggetto erogatore**”).

Ai fini del rilascio della predetta FEA, il Soggetto erogatore si avvale di una soluzione tecnica realizzata da Namirial S.p.A. (di seguito, “**Namirial**”), ente accreditato presso l’Agenzia per l’Italia Digitale (AgID).

La FEA può essere utilizzata esclusivamente in relazione a taluni rapporti da instaurarsi tra il Soggetto erogatore ed i propri dipendenti, dirigenti, amministratori, collaboratori, fornitori e convenzionati i e, segnatamente, per la sottoscrizione dei documenti indicati nelle *Condizioni generali relative al servizio di Firma Elettronica Avanzata* (le “**Condizioni Generali**”), che il firmatario è tenuto ad accettare ai fini dell’attivazione del servizio.

Come descritto nella presente scheda tecnica e nelle predette Condizioni Generali, il processo associato al servizio di Firma Elettronica Avanzata – che prevede l’utilizzo di strumenti di comunicazione a distanza e di una One Time Password (OTP) – garantisce l’identificazione del firmatario del documento, la connessione univoca della firma al firmatario e al documento sottoscritto, il controllo esclusivo del firmatario sul sistema di generazione della firma, la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l’apposizione della firma nonché la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto.

#### **1. Identificazione del firmatario.**

Il Soggetto erogatore, ed i relativi incaricati, identifica in modo certo l’utente firmatario richiedendo il relativo documento d’identità (in corso di validità). Per l’attivazione del servizio di Firma Elettronica Avanzata si procede:

- all’identificazione in modo certo dell’utente tramite un valido documento di riconoscimento in corso di validità di cui viene richiesta copia;
- ad informare il Firmatario in merito agli esatti termini e condizioni relative all’uso del servizio, compresa ogni eventuale limitazione dell’uso (indicata nelle Condizioni Generali);
- a richiedere la sottoscrizione della dichiarazione di accettazione delle condizioni del servizio e a rilasciare idonea informativa relativa al trattamento dei dati personali ai sensi del Regolamento Ue 2016/679 (“GDPR”)
- a richiedere un numero telefonico personale del Firmatario per l’invio dei messaggi SMS di firma con OTP di cui sarà verificata la corrispondenza, nonché un indirizzo e-mail per la trasmissione di documenti e informazioni, come descritto nelle Condizioni Generali che regolano il servizio.

Il processo di identificazione pertanto include l’associazione e la verifica di un numero telefonico in possesso del firmatario, nonché di un indirizzo e-mail del medesimo.

#### **2. Connessione univoca della firma al firmatario**

Il servizio di FEA reso disponibile dal Soggetto Erogatore è supportato dalla piattaforma eSAW (eSignAnyWhere), sviluppata da Namirial.

Il sistema di firma eSAW è progettato per garantire elevati livelli di sicurezza, nonché per rispettare pienamente i requisiti previsti per la Firma Elettronica Avanzata ai sensi della normativa applicabile.

Attraverso il protocollo HTTPS, ogni comunicazione dal sistema di firma eSAW e verso il sistema di firma eSAW è autenticata e protetta. Il sistema eSAW genera un *log* di tutti i passi effettuati e gli eventi registrati, includendo anche gli indirizzi IP e l'eventuale geolocalizzazione del firmatario.

L'integrità del *log* è protetta da sistemi di crittografia basati su firme elettroniche e marche temporali.

### **3. Controllo sul sistema di generazione della firma e processo di sottoscrizione dei documenti**

Al fine di garantire l'associazione univoca tra il firmatario e il dispositivo di Firma Elettronica Avanzata e tra la firma apposta tramite detto dispositivo e il documento sottoscritto:

- i) la documentazione da firmare sarà resa accessibile al Firmatario tramite apposito *link* presente nel testo di una e-mail inviata esclusivamente ad un indirizzo e-mail indicato dal Responsabile e precedentemente verificato;
- ii) per accedere alla documentazione e perfezionare il processo di firma, il Firmatario dovrà inserire nell'interfaccia web presente sulla piattaforma eSAW una *One Time Password (OTP)* – vale a dire, un codice *random* spendibile in un definito arco temporale – inviata via SMS ad un numero di cellulare a lui appartenente, anch'esso verificato in precedenza.

Il cellulare del Firmatario rappresenta, pertanto, il dispositivo di sicurezza abilitante alla firma.

Come descritto nelle Condizioni Generali che regolano il servizio, la soluzione tecnica adottata consente, inoltre, al titolare del dispositivo FEA di:

- visualizzare i contenuti dei documenti al momento della firma così da aver piena evidenza e consapevolezza di quanto sta per sottoscrivere
- ingrandire/rimpicciolire il testo del documento
- individuare agevolmente ogni parte del documento dove è prevista una firma
- confermare la firma apposta
- annullare l'operazione.

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

### **4. Conservazione e sicurezza dei documenti sottoscritti**

Al termine del processo di sottoscrizione, una volta esaurito il processo di cifratura di cui al paragrafo precedente, il documento informatico è inviato al sistema di conservazione, garantendone così l'integrità, l'immodificabilità e la validità nel lungo periodo.

L'integrità del documento informatico 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).

Il sistema utilizza le tecnologie della firma elettronica con chiavi asimmetriche (infrastruttura PKI) e crea documenti in formato standard PAdES (PDF Advanced Electronic Signature), al fine di garantire che non sia possibile nel tempo alterare o modificare il documento informatico sottoscritto dal firmatario e che ogni firma elettronica abbia valore esclusivamente nel contesto del documento per cui è stata generata.

I documenti prodotti dal sistema utilizzano infatti 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).

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.

#### **5. Accesso documentazione relativa al servizio FEA**

Il Soggetto erogatore rende disponibile sul proprio sito internet [www.agoscorporate.it](http://www.agoscorporate.it), nella sezione dedicata alla Firma Elettronica Avanzata, oltre alla presente Scheda Tecnica, la seguente documentazione che deve essere attentamente consultata dal Cliente prima dell'adesione al servizio FEA:

- Condizioni Generali del Servizio FEA (Firma Elettronica Avanzata) e Modulo di adesione
- Informativa ai sensi degli articoli 13 e 14 del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento di dati personali per il servizio di FEA

#### **6. Descrizione della copertura assicurativa**

Al fine di proteggere i soggetti a cui è stata erogata la "FEA" e i terzi da eventuali danni, il Soggetto erogatore e Namirial, in qualità di soggetto che realizza la soluzione tecnica utilizzata per il rilascio della FEA, hanno stipulato appositi contratti di assicurazione per la responsabilità civile.

Più precisamente:

- il Soggetto erogatore ha stipulato con Generali Italia S.p.A. una polizza assicurativa per la copertura della responsabilità civile, per eventuali danni patrimoniali involontariamente cagionati a terzi in conseguenza di un comportamento colposo tenuto dalla medesima o da propri incaricati nell'erogazione di soluzioni di Firma Elettronica Avanzata, avente un massimale non inferiore a euro 750.000 (settecentocinquanta/00);
- Namirial ha stipulato con AIG Europe S.A. una polizza per la copertura della responsabilità civile derivante, *inter alia*, dall'attività di realizzazione e messa a disposizione di soggetti terzi di soluzioni tecnologiche per l'erogazione di soluzioni FEA con un massimale non inferiore a euro 500.000 (cinquecentomila/00).