Manuale Operativo

Manuale Operativo

Firma Elettronica Avanzata FEA

GRAI s.r.l.

Gestione Rischi Agricoli Integrati

Data	Giugno 2018
Versione	2

GRAI Gestione Rischi Agricoli Integrati

Sommario

2 PREMESSA

Il presente documento riporta le informazioni relative al progetto di F.E.A. (Firma Elettronica Avanzata) realizzato dalla società GRAI S.r.l.

3 DEFINIZIONI

3.1 SOGGETTI.

Soggetto	Descrizione
Certificatore	È l'ente, pubblico o privato, abilitato a rilasciare certificati digitali previa specifica procedura di certificazione in conformità con gli standard nazionali ed europei.
Operatore	È la persona incaricata, dal Soggetto che eroga i servizi di Firma Elettronica Avanzata, all'identificazione del cliente; lo informa in merito alle condizioni d'uso e alle modalità del servizio; partecipa al processo di acquisizione della firma elettronica avanzata da parte dell'utente.
Soggetti erogatori dei servizi di firma elettronica avanzata	Sono i soggetti giuridici che erogano soluzioni di firma elettronica avanzata al fine di utilizzarle nei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali, realizzandole in proprio o anche avvalendosi di soluzioni realizzate dai soggetti che le realizzano come attività di impresa.
Soggetti realizzatori dei servizi di firma elettronica avanzata	Sono i soggetti giuridici che, quale oggetto dell'attività di impresa, realizzano soluzioni di firma elettronica avanzata a favore di Soggetti erogatori.
Cliente	È il soggetto a favore del quale la licenziataria mette a disposizione una soluzione di firma elettronica avanzata al fine di sottoscrivere i documenti informatici.

3.2 ACRONIMI.

Sigle	Descrizione
AES	Advanced Encryption Standard è un algoritmo di cifratura a blocchi e a chiave simmetrica operante su un gruppo di bit a lunghezza finita.
AgID	Agenzia per l'Italia Digitale (come da Decreto Legislativo 22 giugno 2012 n.83 articolo 22).
CAD	Il codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n.82 e successivi modificazioni.
Certificato digitale	Nella crittografia asimmetrica un certificato digitale è un documento elettronico che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto (una persona, una società, un computer, etc) che dichiara di utilizzarla nell'ambito delle procedure di cifratura asimmetrica e/o autenticazione tramite firma digitale.
Certificato qualificato	Il certificato digitale conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II del medesima direttiva.
Chiave Privata	È la chiave di crittografia utilizzata in un sistema di crittografia asimmetrica al fine di proteggere la firma apposta. La chiave privata è associata a una chiave pubblica ed è in possesso del Titolare che la utilizza per firmare digitalmente i propri documenti.
Chiave Pubblica	E' la chiave crittografica in un sistema di crittografia asimmetrica ed è utilizzata per verificare la firma digitale apposta su un documento informatico dal titolare della chiave asimmetrica. Tale chiave è associata ad una chiave Privata.
CNIPA (DigitPA)	Centro Nazionale per l'Informatica nella Pubblica Amministrazione. E' l'organismo di controllo istituito dal Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri.

Sigle	Descrizione
Documento Informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Documento analogico	La rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
Firma Elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
Firma Elettronica Avanzata (FEA)	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
Firma digitale	Particolare tipo di firma elettronica basata su un certificato e su un sistema di chiavi crittografiche, pubblica e privata, correlate tra loro, consentendo al titolare, tramite chiave privata, e al destinatario, tramite chiave pubblica, di rendere manifesta e di verificare la provenienza e l'integrità di uno o un insieme di documenti informatici.
HASH	Funzione matematica che genera, a partire da un'evidenza informatica, un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.

Sigle	Descrizione
PAdes	Formato di busta crittografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modifiche.
PDF	È uno standard aperto per lo scambio di documenti elettronici incluso nella categoria ISO (International Organization for Standardization).
RSA	Algoritmo di crittografia asimmetrica. Questo algoritmo si basa su utilizzo di chiavi pubblica e privata.
SHA-1	Acronimo di Secure Hash Algorithm: identifica un algoritmo che genera un'impronta digitale di 160 bit.
SHA-256	Acronimo di Secure Hash Algorithm: identifica un algoritmo che genera un'impronta digitale di 256 bit.
Tablet PC con digitalizzatore	Personal Computer di tipo portatile, dotato di schermo con digitalizzatore e pennino integrato, in grado di acquisire dati biometrici comportamentali e grafici di una firma autografa. I valori acquisiti sono coordinate x-y; tempo; pressione.
Soluzioni di firma elettronica avanzata	Soluzioni strumentali alla generazione e alla verifica della firma elettronica avanzata di cui all'art. 1, comma 1, lettera q-bis del DL 235/2010

3.3 NORMATIVA.

Riferimento	Descrizione
1999/93/CE	Direttiva del Parlamento Europeo e del Consiglio del 13 dicembre 1999 relativa a una comune visione comunitaria in tema di firme elettroniche.
DPR 445/2000	Decreto del Presidente della Repubblica 28 dicembre 2000, n.445 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
D.Lgs. 196/2003	Decreto Legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali".
D.Lgs. 82/2005	Decreto Legislativo 7 marzo 2005 N. 82 "Codice dell'amministrazione Digitale".
D.Lgs. 4 aprile 2006 n. 159	Decreto Legislativo 4 aprile 2006 N. 159.Disposizione integrative e correttive al decreto legislativo 7 marzo 2005, n.82, recante codice dell'amministrazione digitale.
DPCM 12 ottobre 2007	Decreto del Presidente del Consiglio dei Ministri 12 ottobre 2007. Differimento del termine che autorizza l'autodichiarazione circa a rispondenza ai requisiti di sicurezza a cui all'art. 13, comma4, del DPCM, pubblicato sulla Gazzetta Ufficiale del 30 ottobre 2003, n. 13.
DPCM 30 marzo 2009	Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009. Il presente decreto abroga il DCPM del 13 gennaio 2004 "Regole Tecniche" in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici. (Gazzetta Ufficiale n. 129 del 6 giugno 2009).
D.Lgs. 235/2010	Decreto Legislativo 30 dicembre 2010 n. 235. Modifiche ed integrazioni al D.Lgs. 7 marzo 2005 n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge n. 69 del 18 giugno 2009. Codice dell'amministrazione digitale pubblicato su Gazzetta Ufficiale n. 6 del 10 gennaio 2011.
D.Lgs. n.83 22 giugno 2012	Decreto Legislativo n. 83 del 22 giugno 2012 Art 22 Sospensione di CNIPA e DigitPA che confluiscono nell'Agenzia per l'Italia Digitale (AgID).

Riferimento	Descrizione
D.Lgs. N. 221 17 dicembre 2012	Decreto Legislativo n. 221 del 17 dicembre 2012 “Misure Urgenti per la crescita del Paese”. Il CAD, modificato nell’articolo 21, afferma il principio secondo cui “l’utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria”. (la FEA è riportata ai metodi di disconoscimento classici del codice di procedura civile Art 214).
Regole Tecniche DPCM 22 febbraio 2013	Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 “Regole Tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3,24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, 3 e 71.
Provvedimento generale prescrittivo in tema di biometrica – 12 novembre 2014	Provvedimento dell’Autorità Garante del 12 novembre 2014 pubblicato sulla Gazzetta Ufficiale n. 280 del 2 dicembre 2014 che riporta le informazioni e note prescrittive in tema di biometria.
Regolamento UE n. 910/2014	Regolamento eIDAS (electronic IDentification Authentication and Signature) - Regolamento UE n° 910/2014 sull’identità digitale - ha l’obiettivo di fornire una base normativa a livello comunitario per i servizi fiduciari e i mezzi di identificazione elettronica degli stati membri.
D.Lgs. 217/2017	Disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.

4 ATTORI DEL PROGETTO.

4.1 SOGGETTO EROGATORE

GRAI s.r.l. si identifica come Soggetto che eroga la soluzione di firma elettronica avanzata, di tipo grafometrico, al fine di utilizzarla nei rapporti che intrattiene con soggetti terzi (utenti/clienti) per fini prettamente commerciali.

4.1.1 DATI Aziendali

Ragione Sociale: GRAI S.r.l. a socio unico

Indirizzo sede: via Pantano 28, Milano (MI) 20122

Legale Rappresentante: Guido Passarini

Codice Fiscale: 03846420960

Partita IVA: 03846420960

Registro Imprese:Camera di commercio metropolitana di Milano-Monza-Brianza-Lodi

REA: MI-1705603

Capitale Sociale (in Euro): 20.000

Indirizzo E-Mail: amministrazione@grai.it/grai-srl@legalmail.it

Numero Telefonico: 045/8037502

Numero FAX: 045/8000093

Indirizzo Sito Istituzionale: https://www.grai.it

4.1.2 HELP DESK E Servizi di assistenza

Per contattare GRAI s.r.l. al fine di ricevere informazioni e assistenza sul servizio di FEA sono attivi i seguenti punti di contatto:

Via postale: GRAI S.r.l. via da Porto 1, 37122 Verona (VR)

Via e-mail: amministrazione@grai.it

Via telefonica: 045/8037502

Via Fax: 045/8000093

Il servizio è attivo dal lunedì al venerdì dalle ore 9:00 alle ore 18:00

4.2 SOGGETTO CHE REALIZZA LA SOLUZIONE DI FIRMA GRAFOMETRICA

In aderenza a quanto espresso nell'Art, 55 comma 2 lettera b) del DCPM datato 22.2.2013, si segnala che la soluzione di Firma Grafometrica utilizzata da GRAI s.r.l. è stata realizzata dalla società NEOSIGN s.r.l. con sede legale a Savigliano (CN), con omonima soluzione.

4.3 ALTRI SOGGETTI COINVOLTI

4.3.1 Archiva Group s.r.l.

Cura l'attività di archiviazione e conservazione a norma dei documenti digitali sottoscritti con FEA.

4.3.2 Studio Notarile Stucchi-Pini (Torino)

In qualità di Certification Authority fornisce il certificato asimmetrico di crittografia. Conserva inoltre le chiavi private di cifratura del certificato utilizzato per crittografare i dati biometrici delle firme poste sui documenti.

4.3.3 In.Te.S.A. spa

In qualità di Certification Authority fornisce il certificato non qualificato di firma.

5 SCOPO DEL DOCUMENTO

Questo documento si pone lo scopo di descrivere le caratteristiche, le modalità operative, le procedure adottate e le regole predisposte ed utilizzate dagli operatori di GRAI s.r.l. al fine di gestire i servizi di Firma Elettronica Avanzata. Il documento recepisce quanto richiesto dalle Regole Tecniche del 22 febbraio 2013 e dal Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014.

In particolare sono descritte, nel documento, le procedure atte a soddisfare quanto richiesto in tema di generazione, apposizione e verifica della Firma Elettronica Avanzata.
Sono recepite le indicazioni espresse dal D.Lgs. del 7 marzo 2005 e successive modifiche riportate nel D.Lgs. del 30 dicembre 2010, n. 235 e dal DCPM 22 febbraio 2013, Titolo V Firma Elettronica Avanzata.

GRAI s.r.l. provvederà alla verifica della conformità della propria soluzione di Firma Elettronica Avanzata e, qualora si rendesse necessario, provvederà ad aggiornare questo documento anche in considerazione dell'evoluzione della normativa e degli standard tecnologici.

6 FINALITÀ DEL PROGETTO

Con il progetto di Firma Elettronica Avanzata con grafometria, GRAI s.r.l. intende far sottoscrivere ai clienti bollettini di campagna e altri documenti relativi ai prodotti e servizi forniti dalla società stessa. Il poter generare e firmare direttamente in elettronico utilizzando la Firma Elettronica Avanzata permetterà a GRAI di poter dematerializzare i processi cartacei ai fini di una maggiore efficienza, un miglior servizio alla propria clientela ed un maggior rispetto per l'ambiente.

La sottoscrizione di un documento informatico con Firma Elettronica Avanzata con grafo metrica ,
se realizzato nel pieno rispetto di quanto espresso dal DPCM del 22 febbraio 2013 ha l'efficacia prevista all'articolo 2702 del codice civile.

7 LIMITE D'USO

La FEA ha l'efficacia prevista dall'articolo 2702 del Codice Civile e integra il requisito della forma scritta.

Nei documenti normativi citati nel capitolo 3 e con particolare riferimento alle Regole Tecniche, approvate con Decreto del Presidente del Consiglio in data 22 febbraio 2013, si pongono alcune limitazioni all'operatività della Firma Elettronica Avanzata di seguito riassunte:

- La FEA non consente il libero scambio di documenti informatici: il suo uso è limitato al contesto;
- La FEA è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore (Cliente/Utente) e il soggetto che eroga soluzioni di FEA al fine di utilizzarle nel processo di dematerializzazione per motivi istituzionali, societari o commerciali;
- La FEA pur avendo l'efficacia prevista dall'articolo 2702 del Codice Civile presenta alcune eccezioni e in particolare atti di cui l'art. 1350 punti 1-12 del Codice Civile. In questi casi si deve utilizzare la Firma Digitale.

Ai sensi dell'articolo 21 comma 2-bis del CAD sono esclusi, dal poter essere firmati con firma di tipo FEA, i contratti indicati nell'articolo 1350, dal n.1 al n.12 del Codice Civile, ovvero :

1) i contratti che trasferiscono la proprietà di beni immobili;
2) i contratti che costituiscono, modificano o trasferiscono il diritto di usufrutto su beni immobili, il diritto di superficie, il diritto del concedente e dell'enfiteuta;
3) i contratti che costituiscono la comunione di diritti indicati dai numeri precedenti;
4) i contratti che costituiscono o modificano le servitù prediali, il diritto di uso su beni immobili e il diritto di abitazione;
5) gli atti di rinunzia ai diritti indicati dai numeri precedenti;
6) i contratti di affrancazione del fondo enfiteutico;
7) i contratti di anticresi;
8) i contratti di locazione di beni immobili per una durata superiore a nove anni;
9) i contratti di società o di associazione con i quali si conferisce il godimento di beni immobili o di altri diritti reali immobiliari per un tempo eccedente i nove anni o per un tempo indeterminato;
10) gli atti che costituiscono rendite perpetue o vitalizie salve le disposizioni relative alle rendite dello

Stato;
11) gli atti di divisione di beni immobili e di altri diritti reali immobiliari;
12) le transazioni che hanno per oggetto controversie relative ai rapporti giuridici menzionati nei numeri precedenti.

I documenti oggetto di sottoscrizione presso GRAI s.r.l. rispondono quindi a quanto richiesto e posso essere pertanto oggetto di sottoscrizione tramite Firma Elettronica Avanzata.

8 PRIVACY

L'utilizzo di una soluzione di Firma Grafometrica, acquisendo dati biometrici (di tipo comportamentale), ne implica il trattamento. Tali dati biometrici sono cifrati, come descritto nel paragrafo 12 del presente documento.

Tali dati non sono utilizzabili né dal cliente firmatario, né da GRAI s.r.l.

GRAI s.r.l. è titolare del trattamento dei dati e manterrà aggiornato il presente documento, con cadenza annuale.

L'utilizzo dei dati biometrici è funzionale alla firma; non ne viene fatto utilizzo eccessivo in quanto questi dati non sono previsti in consultazione se non in caso di contenzioso sull'autenticità della firma apposta su richiesta di forze dell'ordine o magistratura.

Il processo realizzato prevede la cifratura dei dati, e le chiavi di decifratura sono mantenute dallo **Studio Notarile Stucchi-Pini**, in qualità di Certification Authority, con possibilità di richiesta solo a fronte di contenzioso e richiesta ufficiale dagli organi competenti per l'estrazione, da parte di un perito incaricato dalle parti, in luogo terzo e sicuro.

Considerando che la Firma Grafometrica raccoglie dati biometrici del sottoscrittore è opportuno tener conto dell'articolo 17 e dell'articolo 7 del codice in materia di protezione dei dati personali num. 196/2003.

Art. 17 Trattamento che presenti rischi specifici 1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità di trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti. 2. Le misure e gli accoglimenti di cui a comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.	Il processo realizzato non prevede ne permette la consultazione di dati biometrici acquisiti e, di conseguenza, non permette nessuna analisi di questi dati.
Art. 7 Diritto di accesso ai dati personali e altri diritti 1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile 2. L'interessato ha diritto di ottenere l'indicazione: 2.1 Dell'origine dei dati personali 2.2 Delle finalità e modalità di trattamento	L'interessato sottoscrive una accettazione all'utilizzo della FEA e ha a disposizione una specifica informativa in modo da essere completamente informato sia del processo sia della raccolta dei dati. Potrà inoltre richiedere quanto sottoscritto come esplicitato nel paragrafo 10.5.

9 FIRMA ELETTRONICA AVANZATA

La firma grafometrica è utilizzata per sottoscrivere documenti informatici.

Con il D.Lgs 82/2005 e, successivo, DPCM del 22 febbraio 2013 è stata definita la normativa che regola questa materia e in particolare la Firma Elettronica Avanzata. La Firma Grafometrica è una modalità di firma elettronica che possiede i requisiti tecnici e giuridici tali da poter acquisire la qualifica di Firma Elettronica Avanzata. Il processo di Firma Grafometrica, così come realizzato per GRAI s.r.l. permette al Cliente di firmare documenti informatici che soddisfino i requisiti di sicurezza previsti dalla normativa in essere. Tali documenti hanno lo stesso valore giuridico dei documenti cartacei sottoscritti con firma autografa.

La Firma Grafometrica se conforme all'Art. 1 del CAD (in relazione a quanto introdotto dal decreto legislativo 30 dicembre 2010, n. 235) ed alle Regole Tecniche (art. 56) da questo previste, si pone come Firma Elettronica Avanzata in quanto garantisce questi specifici requisiti (come da Regole Tecniche):

1) L'identificazione del firmatario del documento;
2) La connessione univoca della firma al firmatario;
3) Il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;
4) La possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;
5) La possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;
6) L'individuazione del soggetto di cui all'articolo 55, comma 2, lettera (a) delle Regole Tecniche;
7) L'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatti o dati nello stesso rappresentati;
8) La connessione univoca della firma al documento sottoscritto;

Nello specifico, il processo disegnato per GRAI s.r.l. rispecchia i punti elencati e, di conseguenza, la firma grafometrica adottata si configura come Firma Elettronica Avanzata.

A tale fine, GRAI s.r.l. per rispondere positivamente a quanto richiesto, ha adottato le seguenti misure:

Identificazione del firmatario del documento	L'operatore GRAI segue la medesima operatività prevista per la stipula tramite documento cartaceo. In particolare identifica il firmatario a mezzo dei documenti di riconoscimento in corso di validità.
Connessione univoca della firma con il firmatario	La firma grafometrica permette di acquisire la firma naturale del firmatario e dati vettoriali grafometrici che rendono univoca la firma e potrà essere analizzata con strumenti di verifica a disposizione del perito.
Controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima	La firma apposta unisce 3 strumenti che sono sotto il diretto controllo del firmatario (mano, tablet PC e dati biometrici). L'ambiente è in sicurezza e presidiato e ciò consente di effettuare senza dubbi le verifiche sull'apposizione dei dati biometrici apposti sul documento. In oltre il firmatario può sempre: scorrere il documento; confermare la firma apposta; cancellare la firma apposta e ripetere la firma; annullare l'operazione di firma.
Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma	L'integrità del documento è garantita dal processo che prevede l'apposizione di una firma in formato PAdEs con contestuale generazione di Hash. Esiste sempre la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma. Sul sito di AGID sono presenti i link ad una serie di prodotti per la verifica dei documenti e delle firme (URL : https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/software-verifica), è altresì possibile esigere la verifica con Adobe Acrobat Reader DC.
Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto	Il firmatario ha, sullo schermo del Tablet PC, la visione completa del documento sottoposto a firma e può scorrerlo per analizzarlo. Oltre a ciò il processo prevede la consegna della copia del documento firmato ovvero con trasmissione elettronica dei documenti per mezzo di PEC all'indirizzo fornito dal cliente.
Individuazione del soggetto di cui all'art. 55, comma 2, lettera (a)	GRAI s.r.l. è identificabile come soggetto proponente e ha previsto tutto quanto necessario nel rispetto del requisiti previsti dall'art. 55 comma 2 lettera (a).
Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificare gli atti, fatti o dati nello stesso rappresentati	Il documento generato nel processo di firma è nel formato PDF e sigillato con certificato riconducibile a GRAI s.r.l.

Connessione univoca della firma al documento sottoscritto	Il processo previsto consente quanto richiesto attraverso la generazione di HASH al momento della firma, che può essere utilizzato poi in fase di verifica e controllo. La connessione univoca è garantita dalla soluzione adottata che utilizza algoritmi di cifratura collegate all'impronta del documento.

Tutto ciò nel rispetto dei requisiti richiesti nell'articolo 56 delle Regole Tecniche (DPCM 22/02/2013) e all'articolo 1 (DL 235/2010). In conseguenza di ciò, i documenti informatici sottoscritti dall'utente presso gli operatori di GRAI s.r.l. hanno l'efficacia prevista dall'articolo 2702 del codice civile.

La soluzione adottata risponde positivamente a quanto richiesto, nel documento "Provvedimento generale prescrittivo in tema di biometria – 12 novembre 2014" in tema di sottoscrizione di documenti elettronici a mezzo di biometria.

	PRESCRIZIONE
a)	Il procedimento di firma è abilitato previa identificazione del firmatario.
b)	Sono resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici.
c)	La cancellazione dei dati biometrici grezzi e dei campioni biometrici ha luogo immediatamente dopo il completamento della "procedura di sottoscrizione" e nessun dato biometrico persiste all'esterno del documento informatico sottoscritto.
d)	I dati biometrici e grafometrici non sono conservati, neanche per periodi limitati, sui dispositivi hardware utilizzati per la raccolta, venendo memorizzati all'interno dei documenti informatici sottoscritti in forma cifrata tramite sistemi di crittografia a chiave pubblica.
e)	La trasmissione dei dati biometrici tra sistemi hardware di acquisizione, postazioni informatiche e server avviene esclusivamente tramite canali di comunicazione resi sicuri con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita.
f)	Sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione delle postazioni informatiche e dei dispositivi, se non esplicitamente autorizzati.
g)	I sistemi informatici sono protetti contro azioni di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati.
h)	Nel caso di utilizzo di sistemi di firma grafometrica nello scenario mobile o BYOD (Bring Your Own Device). Sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili, con il ricorso a strumenti MDM (Mobile Device Management) o MAM (Mobile Application Management) o altri equivalenti al fine di isolare l'area di memoria dedicata all'applicazione biometrica, ridurre i rischi di installazione abusiva di software anche nella caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (malware).
i)	I sistemi di gestione impiegati nei trattamenti grafometrici adottano certificazioni digitali e policy di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro (in particolare, rendendo disponibili funzionalità remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi).
j)	L'accesso al modello grafometrico cifrato avviene esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, o da più soggetti, in caso di frazionamento della chiave stessa, e nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma a seguito di richiesta dell'autorità giudiziaria. Le condizioni e le modalità di accesso alla firma grafometrica da parte del soggetto terzo di fiducia o da parte di tecnici qualificati sono dettagliate nell'informativa resa agli interessati e nella relazione tecnica successivamente citata.
k)	Il documento corrente descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento del dato biometrico rispetto alle finalità. Il documento è conservato ed aggiornato, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuto a disposizione del Garante.

10 OBBLIGHI DEL SOGGETTO EROGANTE

I soggetti che erogano soluzioni FEA hanno una serie di obblighi al fine di mantenere tutti i requisiti richiesti dal DL 235/2010 Art. 1 e dell'articolo 57 del DPCM 22/02/2013 che di seguito sono riassunti e nei paragrafi successivi descritte e dettagliate.

1) Identificare in modo certo l'utente tramite un valido documento di riconoscimento;
2) Informare l'utente in relazione agli esatti termini e condizioni d'uso del servizio, compresa ogni eventuale limitazione d'uso;
3) Subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente;
4) Conservare per almeno **20 anni** copia del documento di riconoscimento e la dichiarazione del punto 3;
5) Garantire la disponibilità, integrità, leggibilità e autenticità del documento di accettazione del servizio (punto 3);
6) Fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui al punto 3) al firmatario su sua richiesta;
7) Rendere note le modalità con cui effettuare la richiesta di cui al punto 6), pubblicandole anche sul proprio sito internet;
8) Rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dalle Regole Tecniche articolo 56, comma 1;
9) Specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto;
10) Prevedere la possibilità di revoca del servizio da parte del cliente/utente.

10.1 IDENTIFICAZIONE DEL FIRMATARIO

L'identificazione del firmatario viene effettuata dagli operatori di GRAI s.r.l.; a tal fine vengono richiesti documenti di identità e codice fiscale. Tutti i documenti debbono essere in corso di validità.

Per quanto concerne i documenti di riconoscimento, come da articolo 35 del DPR 445/2000, sono considerati validi i seguenti:

- ✓ Carta d'identità
- ✓ Passaporto
- ✓ Patente di Guida
- ✓ Patente Nautica
- ✓ Libretto della Pensione
- ✓ Patentino di abilitazione alla conduzione di impianti termici
- ✓ Porto d'Armi

10.2 INFORMAZIONI PER IL FIRMATARIO

Gli operatori di GRAI s.r.l., prima di procedere con la richiesta di accettazione dell'utilizzo del servizio FEA, procedono a informare il firmatario in relazione alla finalità (come espresso nel capitolo 6) le limitazioni d'uso (capitolo 7). Viene anche presentata e, se richiesta, consegnata, informativa dettagliata per l'utilizzo del servizio.

10.3 DICHIARAZIONE DI ACCETTAZIONE

Gli operatori di GRAI s.r.l. dopo aver adeguatamente informato il cliente firmatario, chiedono la sottoscrizione della dichiarazione di accettazione delle condizioni di erogazione del servizio da parte del cliente. Tale documento riporta tutti i dati informativi del cliente, la descrizione del servizio e richiede firme digitali su documento digitale per l'accettazione del servizio, modifiche di rapporto e consenso alla raccolta dei dati biometrici.

10.4 CONSERVAZIONE DOCUMENTI

In pieno rispetto di quanto previsto nell'articolo 56 comma 1 del DPCM 22/02/2013, al fine di dare evidenza di quanto previsto, si eseguono copia del documento di riconoscimento e del codice fiscale. Queste copie, in allegato al documento di accettazione del servizio, verranno conservate per almeno 20, anni da GRAI s.r.l. garantendone, per tutto il periodo richiesto la disponibilità, integrità e leggibilità.

10.5 DISPONIBILITÀ DEI DOCUMENTI SOTTOSCRITTI DAL CLIENTE

Su richiesta del cliente effettuata mediante comunicazione scritta, GRAI s.r.l. si rende disponibile a fornire, senza oneri per il cliente, copia cartacea della dichiarazione di accettazione da parte del Cliente stesso delle condizioni e dei termini del Servizio oltre alle copie dei documenti firmati con FEA e conservati in copia senza la presenza dei dati biometrici al solo scopo di informazione.

Il cliente potrà contattare GRAI s.r.l. per ricevere assistenza per attivare la richiesta.

10.6 CARATTERISTICHE DEL SISTEMA DI FIRMA

Al fine di ottemperare alla normativa di cui articolo 56 comma 1, GRAI s.r.l., nel paragrafo 12 descrive le misure adottate a garanzie di quanto prescritto.

10.7 TECNOLOGIA UTILIZZATA

Nel paragrafo 13, GRAI s.r.l., descrive in modo dettagliato le caratteristiche hardware e software al fine di ottemperare quanto richiesto dalle Regole Tecniche DPCM 22/02/2013.

10.8 PUBBLICAZIONE SUL SITO

GRAI s.r.l., in ottemperanza a quanto richiesto dalla normativa in essere, ha pubblicato sul sito internet www.grai.it il presente documento che descrive anche le caratteristiche del sistema di firma e le caratteristiche delle tecnologie utilizzate.

10.9 SERVIZIO DI REVOCA

Il processo di Firma Elettronica Avanzata adottato da GRAI s.r.l. permette la revoca dei servizi tramite apposita richiesta scritta da parte del cliente. In caso di revoca la FEA non potrà più essere utilizzata.

Il cliente potrà contattare GRAI s.r.l. per ricevere assistenza per attivare le richiesta di Revoca.

11 TUTELA ASSICURATIVA

Ulteriore richiesta espressamente citata nelle Regole Tecniche, prevede una copertura assicurativa a garanzia del firmatario. In particolare, nelle Regole Tecniche art. 57 comma 2, si cita che:

Il soggetto che eroga soluzioni di Firma Elettronica Avanzata si impegna a stipulare una polizza assicurativa, con società abilitata ad esercitare nel campo dei rischi industriali, per la copertura dei rischi dell'attività svolta e dei danni a tutela delle parti (Firmatari ed i Terzi) per almeno Euro 500.000,00(cinquecentimila/00).

GRAI s.r.l., in qualità di soggetto che eroga la soluzione di Firma Elettronica Avanzata, ha stipulato polizza assicurativa con primaria compagnia Assicurativa abilitata ad esercitare nel campo dei rischi industriali, per la copertura dei rischi dell'attività svolta e dei danni a tutela delle parti.

12 LA SOLUZIONE GRAI s.r.l.

12.1 IL SOFTWARE DI FIRMA

Per la realizzazione del servizio di Firma Elettronica Avanzata con Firma Grafometrica, GRAI s.r.l. ha utilizzato il software NEOSIGN, appositamente installato sulla postazione degli operatori della società stessa. NEOSIGN è prodotto dalla omonima società NEOSIGN s.r.l. avente sede a Savigliano (CN).

12.2 IL CLIENT NEOSIGN

E' la componente installata sui Tablet PC degli operatori ed ha il compito di ricevere e visualizzare i documenti da sottoporre all'utente firmatario, di acquisire i dati biometrici, di cifrarli insieme ad altre informazioni (chiave AES cifrata, tratto grafico e dati del PC) e di inserirli all'interno del documento PDF.

Il Client NEOSIGN rende il documento non modificabile grazie all'apposizione di una firma Pades, e tramite apposito certificato rilasciato da una Certification Authority accreditata presso AgID (Intesa spa).

Il Client NEOSIGN, per la cifratura delle informazioni, utilizza due differenti algoritmi di cifratura , un primo algoritmo di cifratura simmetrica AES per cifrare i dati biometrici dell'utente; un secondo algoritmo di cifratura asimmetrica RSA (chiave pubblica) per cifrare la chiave AES. La chiave AES è generata in maniera casuale dal Client per ogni firma. La chiave pubblica di cifratura utilizzata dall'algoritmo RSA è distribuita insieme al Client di firma NEOSIGN.

12.3 MODALITÀ DI FIRMA

La soluzione prevede l'installazione del Client di firma sui Tablet PC degli operatori di GRAI s.r.l.

L'installazione di tale Client è curata direttamente dal personale tecnico di GRAI s.r.l.

La prima attività che viene richiesta al cliente, in modo che possa poi usufruire dei servizi di FEA, è l'accettazione e sottoscrizione del consenso all'utilizzo della FEA e alla raccolta dei dati biometrici. Tale consenso viene raccolto dall'operatore dopo aver fatto leggere l'informativa al cliente.

Per la sottoscrizione di documenti digitali da parte degli utenti, è necessario che l'operatore, sempre presente alle sottoscrizioni, abbia inserito le proprie credenziali d'accesso sul proprio PC, e debba essere stato riconosciuto dal sistema informativo di GRAI s.r.l.

All'utente firmatario sono quindi sottoposti documenti digitali in formato PDF con uno o più campi firma; il campo firma viene presentato al sottoscrittore in modalità esplicita sul Tablet PC e l'intero foglio del documento è disponibile e visualizzato sullo stesso.

L'utente firma direttamente sullo schermo del Tablet PC, avendo la percezione di una classica firma sulla carta, mantenendo il controllo esclusivo dell'operazione di firma.

Premendo quindi il tasto OK il Cliente accetta l'invio dei dati biometrici che sono immediatamente acquisiti dal Client NEOSIGN, cifrati, ed inseriti nel documento.

A seguito dell'apposizione di ogni singola firma il documento viene sigillato con un certificato non qualificato di chiusura a nome dell'azienda. Il documento sigillato con il certificato di chiusura viene poi messo a disposizione del servizio di archiviazione e conservazione a norma fornito da Archiva Group s.r.l.

In caso di non conferma, il documento viene cancellato dalla memoria del sistema.

12.4 LA SICUREZZA

In tema di firma grafometrica, sono state adottate particolari attenzioni alla sicurezza del dato biometrico acquisito. Infatti, mentre il firmatario esegue la firma, i dati biometrici che lo caratterizzano sono cifrati nella memoria del PC con la chiave simmetrica AES, la cui chiave a sua volta è cifrata con la chiave pubblica tramite l'algoritmo asimmetrico RSA.

Il firmatario ha il controllo esclusivo del processo di firma disponendo di una serie di funzioni e può:

- Scorrere il documento senza limitazioni al fine di poter aver evidenza di quanto da lui sarà sottoscritto;
- Firmare con apposita penna sullo schermo del Tablet PC nell'apposita area di firma;
- Confermare la firma apposta selezionando il pulsante **OK** dopo aver apposto la firma;
- Cancellare la firma apposta qualora non sia, a suo avviso, soddisfacente utilizzando il pulsante **RIPROVA** e poi ripetere la firma;
- Annullare l'operazione di firma qualora non sia più disposto a firmare il documento, selezionando il pulsante **ANNULLA**.

Con la conferma (**pulsante OK**) da parte del firmatario alla firma apposta il programma effettua il calcolo dell'impronta del documento con l'algoritmo SHA.

I dati biometrici cifrati, la chiave AES cifrata, il tratto grafico, dati del PC utilizzato e l'impronta (HASH) del documento, sono inseriti nel documento PDF, alla fine del processo di firma, in standard PAdES, secondo la deliberazione CNIPA 21 maggio 2009, n.45.

Quest'ultima firma, garantisce l'integrità (documento non alterato) e autenticità (autore) del documento digitale (GRAI s.r.l.).

I dati biometrici così protetti non possono essere decriptati, visualizzati ed esaminati. Unica possibilità è di poter disporre della chiave privata, chiave in possesso solo di ente terzo e con regole di consegna solo per particolari eventi, e di un apposito software di analisi.

Questa operazione è prevista come processo di gestione di eventuali contenziosi.

12.5 INTEGRITÀ DEL DOCUMENTO SOTTOSCRITTO

L'integrità del documento sottoscritto dall'utente è garantita dalla firma PADEs apposta in chiusura di ogni singola firma.

L'apposizione di tale firma è gestita direttamente dal Client NEOSIGN.

Il Client calcola l'impronta del documento, che cifra con i dati biometrici e che quindi inserisce nel documento.

Il risultato del processo è la firma del documento che ne garantisce l'integrità e autenticità.

La verifica dell'integrità ed autenticità del documento può essere svolta da un qualsiasi software di verifica conforme al CAD; ad esempio ADOBE ACROBAT READER DC.

La verifica dell'autenticità della sottoscrizione (la firma) dell'utente può essere eseguita solo quando si è in possesso della chiave privata di cifratura.

La chiave privata di cifratura è conservata presso un ente terzo fidato, **Studio Notaio Stucchi** in questo caso, che renderà disponibile la chiave solo su motivata (es. l'autorità giudiziaria) richiesta del legale rappresentante.

13 HARDWARE DI FIRMA

GRAI s.r.l. ha deciso di dotare i propri operatori, al fine di erogare i servizi ai clienti, di un tablet PC di tipo **Acer Switch 12, Acer Switch 5 oppure Dell Venue 11 Pro**

Di seguito sono riportate le principali caratteristiche tecniche:

Acer Switch 12

Operating	System Windows 10 Home
Processor	Intel® Core™ i3-6100U 2.3 GHz; Dual-core
Memory	LPDDR3 4 GB (standard)
Card Reader	microS microSDXC
Storage	128 GB SSD
Screen	12" QHD (2160 x 1440) resolution multi-touch IPS technology
Graphics	Intel® LPDDR3 Shared graphics memory
Connectivity	802.11ac wireless LAN Bluetooth 4.0
Audio & Video	Two speakers 1MP (Front camera) 1MP auto focus (Rear camera)
Ports& Connectors	1x USB 3.1 Type-C
Input Devices	TouchPad, Stylus
Battery	2-cell 4870 mAh Li-Polymer
Battery	Life 8 hours
Adapter	45 W
Dimensions (W x D x H)	292.10 mm x 201.40 mm x 15.85 mm
Weight (Approximate)	1.25 kg (with dock)

Acer Switch 5

Sistema Operativo	Windows 10 Pro
Processore	Intel® Core™ i5-7200U
	2,5 GHz; Dual-core
Memoria	LPDDR3 - 8 GB
Lettore di schede	microSD, microSDXC
Archiviazione	256 GB SSD
Display	12", TXGA (2160 x 1440) resolution, 10-point Multi-touch,
	Tecnologia IPS
Grafiche	Intel® HD Graphics 620, LPDDR3 condivisa memoria grafica
Connettività	802.11ac LAN wireless, Bluetooth 4.0
Audio e video	1600 x 1200 webcam, Digitale Microfono, 1 x Speaker, 1MP
	(Fotocamera frontale), 1MP Auto focus (Fotocamera
	posteriore)
Porte e connettori	1x USB 3.0, 1x USB 3.1 Gen 1 Type-C
Dispositivi input	TouchPad, Stilo
Retroilluminato tastiera	
Batteria	2-cell 4870 mAh Polimeri di litio
Adattatore	45 W
Dimensioni (L x P x H)	292,90 mm x 201,80 mm x 9,60 mm
	292,90 mm x 201,80 mm x 15,95 mm
Peso (approssimativo)	1,27 kg (con docking)

Dell Venue 11 Pro

Display	10.8 inch TFT Display with FHD (1920 x 1080) resolution, 400
	nits and 10-pt capacitive
touch	
Processors	Intel® Core™ M 5Y10c processor (4MB L3 Cache, 2.0 GHz Dual
	-Core) / Intel® Core™ M vPro 5Y71 processor (4MB L3 Cache,

	2.9 GHz Dual -Core)
Operating System	Windows™ 8.1 (64-bit) / Windows™ 8.1 Pro (64-bit)
Memory	4GB or 8GB LPDDR3 1600MHz
Storage	64GB, 128GB or 256GB Solid State Storage
Graphics	Intel® HD Graphics 5300
Audio	MaxxAudio® by Waves
Wireless	Intel® 7265 Dual-Band 2x2 802.11 ac WiFi (Miracast) Bluetooth® 4.0 Mobile Broadband 4G (LTE) Mobile Broadband Card Telit LN930-LTE –M.2, USB2, (Intel XMM 7160) (LTE/HSPA+) Mobile Broadband Card
Cameras	Integrated 2MP HD Webcam (front) / 8MP (back)
Security	Intel® Platform Trust Technology, Trusted Platform Module (TPM) 1.2 (optional) Chassis lock slot support
Ports and Connectors	Micro-SD Card Reader (SD, SDHC, SDXC, supporting up to 64GB) 1 x Full size USB3.0 Headphone and microphone combo jack 1 x micro HDMI BT4.0, NFC (optional) Sensor Hub (Gyro, G-sensor, Proximity),
Dimensions	Width: 11.01” / 279.8mm Depth: 0.42”/ 10.75mm Height (front/back): 6.95”/176.4mm
Battery	38Whr Lithium Ion battery
Weight	722.6g (1.59lb) WLAN; 747.7g (1.65lb) WWAN
Power Adaptor	24 Watt AC adapter (micro USB charging)

14 ALTRE COMPONENTI

Per la realizzazione di un processo di firma in piena conformità con le Regole Tecniche emesse il 22/02/2013 con Decreto del Presidente del Consiglio dei Ministri, sono necessari i componenti di seguito descritti.

CHIAVE PUBBLICA DI CIFRATURA

I dati biometrici sono cifrati utilizzando una chiave simmetrica generata dal software di firma, questa chiave è cifrata con chiave pubblica di cifratura. La chiave pubblica è distribuita da NEOSIGN insieme al programma Client ed è generata dallo Studio Notarile Stucchi, in qualità di Certification Authority.

CHIAVE PRIVATA DI CIFRATURA

La chiave privata, unica in grado di estrarre in chiaro i dati di firma è generata dallo Studio Notarile Stucchi in qualità di Certification Authority. Lo Studio sarà chiamato, in fase di eventuale contenzioso, dall'autorità giudiziaria seguendo il processo previsto per la gestione del contenzioso e illustrato in questo documento.

CERTIFICATO DI FIRMA

Il certificato di firma è installato sulle postazioni degli operatori, ed è utilizzato al termine del processo di Firma Elettronica Avanzata, al fine di garantirne l'integrità (documento non alterato) ed autenticità del documento digitale.

15 ARCHIVIAZIONE E CONSERVAZIONE A NORMA DEI DOCUMENTI

Il processo di archiviazione e conservazione a norma è a carico di Archiva Group s.r.l. che provvederà alla stesura del "Manuale di Conservazione" e assumerà la responsabilità della conservazione a norma per le sue componenti.

16 GESTIONE DEL CONTENZIOSO

Il processo di gestione di un contenzioso, inizialmente segue le classiche politiche di gestione previste dalla società ma, in ipotesi che il contenzioso veda l'intervento di giudici per risolverlo, si deve obbligatoriamente prevedere un diverso approccio di perizia.

In particolare è necessario procedere ad una perizia dei dati informatici e biometrici delle firme in contenzioso.

Per questo motivo NEOSIGN mette a disposizione un software che permette l'analisi dei dati biometrici e informatici della firma nonché la visione delle modalità di generazione della firma a mezzo di una ricostruzione utilizzando i parametri memorizzati.

Ovviamente per poter effettuare questo controllo è indispensabile poter accedere ai dati crittografati della firma.

In sintesi il processo prevede:

a) Viene definito dagli organi giudiziari il perito incarica della perizia;

b) L'autorità giudiziaria definisce la sede dove si svolgerà la perizia (tribunale; ufficio del perito; sede della Certification Authority o altra sede) ed i tempi di effettuazione della perizia;

c) Viene richiesto, alla società di conservazione, l'originale elettronico del documento contestato contenente le firme;

d) Nella sede individuata la Certification Authority (o la/le risorse indicate come referenti) rende disponibile la chiave di decifratura, ed inserisce la password per permettere di accedere alla chiave stessa, che sarà utilizzata nel sistema di perizia fornito dalla società NEOSIGN;

e) Il perito analizza i dati informatici e biometrici delle firme apposte, confrontando i dati con altri documenti firmati entro un periodo di un anno.