



MANUALE OPERATIVO

**Descrizione Tecnica della soluzione di
Firma Elettronica Avanzata in modalità grafometrica**



Sommario

1	<u>INTRODUZIONE</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
1.1	<u>SCOPO</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
1.2	<u>NORMATIVA DI RIFERIMENTO</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
2	<u>DESCRIZIONE DELLA SOLUZIONE DI FIRMA GRAFOMETRICA</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
3	<u>REQUISITI DI SICUREZZA</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
3.1	<u>COMPLIANCE NORMATIVA</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
4	<u>PROCESSO DI FIRMA GRAFOMETRICA</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
4.1	<u>AMBITO DI UTILIZZO</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
4.2	<u>RUOLI FUNZIONALI</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
4.3	<u>IDENTIFICAZIONE DEL/I FIRMATARIO/I ED ADESIONE AL SERVIZIO DI FIRMA GRAFOMETRICA</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
4.4	<u>PROCESSO DI SOTTOSCRIZIONE DEL DOCUMENTO INFORMATICO</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
4.4.1	<u>Flusso Operativo</u>	<i>Errore. Il segnalibro non è definito.</i>
5	<u>CARATTERISTICHE DEL SERVIZIO E DELLE TECNOLOGIE UTILIZZATE</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
5.1	<u>APPLICAZIONE CLIENT DESKTOP STANDALONE</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
5.2	<u>PROTEZIONE DEI DATI BIOMETRICI</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
5.3	<u>TABLET/PAD MANAGER – STANDARD BIOMETRICI UTILIZZATI</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
5.4	<u>PDF MANAGER E GESTIONE PDF</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
5.5	<u>GESTIONE DELLE LICENZE DELLE COMPONENTI SOFTWARE</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
6	<u>REQUISITI NORMATIVI</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.

Indice delle Tabelle

<u>TABELLA 1: REQUISITI DI SICUREZZA</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
<u>TABELLA 2: COMPLIANCE NORMATIVA</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
<u>TABELLA 3: PROCESSO DI FIRMA</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.
<u>TABELLA 4: REQUISITI NORMATIVI</u>	ERRORE. IL SEGNALIBRO NON È DEFINITO.

1 INTRODUZIONE

PROGETTO DI DEMATERIALIZZAZIONE DOCUMENTALE E SEMPLIFICAZIONE PROCESSI

Per l'erogazione di tale servizio **Zanesi S.r.l.** ha deciso di inserire nel progetto di dematerializzazione e di semplificazione dei processi che sta perseguendo, anche la digitalizzazione di tali disposizioni attraverso la predisposizione di documenti informatici (documenti informatici) che potranno essere firmati dagli interessati attraverso la Firma Elettronica Avanzata (FEA) in modalità grafometrica, con trattamento e conservazione dei dati biometrici.

La firma potrà essere apposta sia dagli utenti che dagli Operatori che presenziano la dichiarazione da parte degli utenti.

Tale procedura permette di evitare l'archiviazione di documenti in formato cartaceo.

1.1 Scopo

Il presente Manuale Operativo descrive gli obblighi, le garanzie, le responsabilità, procedure operative e, in generale, le caratteristiche che rendono affidabile il processo di apposizione di una firma elettronica avanzata grafometrica (di seguito anche "Servizio") adottato da **Zanesi S.r.l.** come alternativa alla tradizionale firma autografa e tramite cui il contraente aderisce ai servizi offerti.

Il presente documento, reperibile, consultabile ed estraibile in formato elettronico sul sito web del soggetto Erogatore alla pagina <https://www.zanesi.it/fea>, è redatto in conformità a quanto previsto dall'articolo 57, commi 1 e 3, del D.P.C.M. 22 febbraio 2013 (DPCM), attuativo del Codice dell'Amministrazione Digitale di cui al D.Lgs. n. 82/2005 (CAD) e recante le regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.

Sono recepite le indicazioni espresse dal Titolo V del DPCM e dal CAD in materia di firma elettronica avanzata.

1.2 Normativa di riferimento

- [1] *Decreto del Presidente del Consiglio dei Ministri (DPCM) 22 febbraio 2013, "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali", GU n.117 del 21 maggio 2013.*
- [2] *Decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il Codice dell'amministrazione digitale (CAD).*

2 DESCRIZIONE DELLA SOLUZIONE DI FIRMA GRAFOMETRICA

Il processo di Firma Elettronica Avanzata (di seguito "FEA") utilizzato da **Zanesi S.r.l.** è basato sull'utilizzo della firma grafometrica e prevede l'apposizione della firma autografa da parte dell'utente su una tavoletta grafometrica attraverso un'apposita penna elettronica ad essa collegata.

La tavoletta, collegata ad una postazione PC desktop, rileva alcuni dati biometrici di tipo comportamentale dell'utente quali velocità, pressione, ritmo, accelerazione e movimento.

Questi dati biometrici sono utilizzati per attribuire **univocamente** la firma apposta al soggetto che l'ha eseguita attraverso apposito software.



Tale soluzione di Firma Grafometrica consente di creare un documento informatico che contiene al suo interno tutti gli elementi necessari a stabilirne l'autenticità, essendo formato dal contenuto del documento sottoscritto e dai dati biometrici cifrati, relativi alla sottoscrizione da parte dell'utente.

I dati biometrici non sono in alcun modo memorizzati e conservati, ma sono raccolti e rimangono esclusivamente all'interno del documento informatico, cifrati al fine di impedirne il riuso o una loro elaborazione che porti a falsificare o riprodurre la firma su altri documenti.

La chiave di decifratura è conservata, con elevati livelli di sicurezza, presso la Certification Authority Aruba PEC S.p.A. con sede legale in via San Clemente n° 53 – 24036 Ponte San Pietro (BG).

La cifratura dei dati biometrici avviene attraverso un certificato di protezione dei dati biometrici emesso da Aruba PEC in qualità di Certification Authority composto da:

- Una parte pubblica che cifra;
- Una parte privata che decifra.

La chiave pubblica viene fornita al **Zanesi S.r.l.** ed è installata sul client. La chiave privata, l'unica capace di gestire in chiaro i dati biometrici, è conservata da Aruba PEC in qualità di ente terzo garante, essendo Aruba PEC Certification Authority accreditata presso AgID.

Esattamente come per un documento cartaceo, nel caso di contenzioso o ripudio della firma da parte del sottoscrittore sarà necessario effettuare una perizia calligrafa, verificando attraverso la strumentazione in dotazione le caratteristiche della firma, mediante il confronto tra il documento in analisi che contiene la firma, ed i dati biometrici raccolti da un perito calligrafo o altro esperto del settore.

Solo in questo caso si potrà utilizzare la chiave di decifratura ed accedere ai dati biometrici contenuti nel documento oggetto di contenzioso.

Il soggetto erogatore del servizio di Firma Grafometrica è il **Zanesi S.r.l.**

3 REQUISITI DI SICUREZZA

La Soluzione di firma grafometrica adottata da **Zanesi S.r.l.** si basa sulla libreria **AGI (Aruba Graphometric Interface)**.

Tale software consente, in combinazione con **opportuni dispositivi hardware** e con **opportune procedure operative** in capo all'Organizzazione che lo utilizza, di implementare una completa soluzione di Firma Elettronica Avanzata (FEA) *conforme ai requisiti della normativa vigente*, con particolare riferimento all'*art. 56 del DPCM 22/2/2013*.

Questo implica che il software (e soprattutto la libreria) possieda delle caratteristiche di sicurezza tali da soddisfare i seguenti requisiti:

ID	Requisito (Art. 56 del DPCM 22/02/2013)
RQ1	Identificazione del firmatario del documento.
RQ2	Connessione univoca della firma al firmatario.
RQ3	Controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma.
RQ4	Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma
RQ5	Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto
RQ6	Individuazione del soggetto che ha erogato la soluzione di firma elettronica avanzata
RQ7	Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati
RQ8	Connessione univoca della firma al documento sottoscritto.

Tabella 1: Requisiti di Sicurezza

Le caratteristiche di sicurezza del software rispecchiano in toto quelle offerte dalla libreria AGI. Tali caratteristiche, meglio descritte più avanti nel presente documento, possono però essere riassunte nelle seguenti **funzionalità essenziali della libreria AGI**:

- I **dati biometrici** della firma sono **inseriti nel documento in forma cifrata** mediante crittografia asimmetrica RSA, usando una chiave specificamente dedicata a tale operazione;
- La **chiave privata** di decifratura (cui corrisponde la chiave pubblica indicata al punto precedente) viene **custodita da una terza parte fidata**, nel caso specifico presso la CA Aruba PEC, e non è normalmente acceduta da nessuno (custodita in modalità "off-line") tranne che dalle Autorità in caso di contenzioso;
- I dati che vengono cifrati ed inseriti nel documento includono non solo i parametri biometrici della firma ma **anche l'impronta (hash) del documento stesso**;
- Dopo l'apposizione delle necessarie firme grafometriche (una o più), **il documento viene "sigillato" mediante una firma digitale qualificata** dell'Operatore del **Zanesi S.r.l.**

Nei paragrafi successivi sono descritte le funzionalità della Soluzione di Firma Grafometrica.

3.1 Compliance Normativa

Di seguito vengono riepilogati i prerequisiti previsti dalla normativa sulla Firma Elettronica Avanzata e come questi sono soddisfatti dalle caratteristiche della soluzione di Firma Grafometrica proposta da Aruba PEC:

Requisito (Art. 56 del DPCM 22/02/2013)	Rif -Razionale
Identificazione del firmatario del documento.	L'identificazione del firmatario avviene al momento della presenza del sottoscrittore dinnanzi all'Operatore di Zanesi S.r.l.
Connessione univoca della firma al firmatario.	La connessione univoca al firmatario avviene grazie al meccanismo di "document binding" che prevede la raccolta dell'hash del documento uniti ai parametri grafometrici di quella firma e la loro cifratura con chiave pubblica di Aruba PEC. Il legame, costruito tramite sistema di cifrature, impedisce che il blob di firma possa essere estratto e riutilizzato su un altro documento in quanto resta sempre riconducibile all'unico documento cui è collegato, firmato originariamente dal cliente.
Controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma.	La soluzione di firma proposta si basa sull'acquisizione dei dati grafometrici/comportamentali statici e dinamici legati all'azione della sottoscrizione, quale elemento sul quale il firmatario mantiene un controllo esclusivo. Inoltre il software Aruba PEC è progettato per evitare che ci sia un doppio utilizzo (accidentale o malevolo) dello stesso set di dati grafometrici.
Possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma	A garanzia dell'integrità e immutabilità del documento viene ricalcolata la rappresentazione numerica del documento, successiva all'apposizione dei dati di firma (nuovo "hash") e il documento viene "chiuso" con firma elettronica non qualificata della postazione. In questo modo, il documento è reso "non modificabile". L'eventuale alterazione è facilmente verificabile anche con programmi di lettura di documenti di comune diffusione quale Adobe Reader il quale, in caso di modifica di un documento post firma elettronica, ne evidenzia l'alterazione.
Possibilità per il firmatario di ottenere evidenza di quanto sottoscritto	Il sistema AGI mette a disposizione le funzioni che, completata la firma grafometrica, permettono di recuperare in diverse modalità copia elettronica del documento sottoscritto.
Individuazione del soggetto che ha erogato la soluzione di firma elettronica avanzata	L'individuazione del soggetto che ha erogato il servizio di FEA è implementato grazie all'apposizione della firma di integrità e alla firma elettronica qualificata di chiusura del documento da parte dell'Operatore di Zanesi S.r.l.

Requisito (Art. 56 del DPCM 22/02/2013)	Rif -Razionale
<p>Assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati</p>	<p>Il documento prodotto è in un formato tale da impedire l'inserimento all'interno dello stesso di programmi o istruzioni potenzialmente atti a modificare gli atti, fatti o dati rappresentati nel documento medesimo.</p> <p>Inoltre la libreria AGI prevede controlli preventivi alla firma grafometrica che servono per rilevare la presenza di componenti dinamici in grado di modificare gli atti o i fatti rappresentati e impedire la generazione del documento firmato grafometricamente.</p>
<p>Connessione univoca della firma al documento sottoscritto.</p>	<p>Al fine di garantire la connessione univoca della firma al documento, l'applicazione di firma:</p> <ul style="list-style-type: none"> • calcola per il documento generato dalla transazione, prima dell'apposizione sullo stesso della firma l'hash quale elemento univoco di identificazione del documento prodotto; • riceve dalla tavoletta in maniera sicura (criptandoli) i dati biometrici della firma (sia "statici" che "dinamici") e li abbina alla stringa calcolata in precedenza, creando il c.d. G-blob; • "chiude" e cifra il G-blob, la cui decodifica può avvenire solo tramite un sistema di "chiavi" di cui una detenuta dall'Organizzazione (denominata "chiave pubblica") ed una conservata a cura di un soggetto terzo rispetto alla Organizzazione (denominata "chiave privata"). Il soggetto terzo che detiene la chiave privata è Aruba PEC; • infine, sul documento ottenuto, nel quale esiste un riferimento cifrato sia al documento precedente la firma (stringa alfanumerica) che al firmatario (dati biometrici), calcola un nuovo hash e "chiude" il documento mediante certificato di firma digitale (o comunque mediante certificato di firma elettronica qualificata) <p>Il suddetto legame costruito tramite sistema di cifrature, impedisce che il G-blob di firma possa essere estratto e riutilizzato su un altro documento in quanto resta sempre riconducibile all'unico documento cui è collegato, firmato originariamente dal cliente.</p> <p>Il documento potrà essere decifrato, in caso di necessità, per l'esibizione in giudizio o su richiesta dell'autorità giudiziaria, su richiesta del cliente o per esigenze dell'Organizzazione per la verifica dell'integrità del contenuto dello stesso e della paternità della firma apposta, solo con il concorso del possessore della chiave "privata".</p>

Tabella 2: Compliance Normativa

4 PROCESSO DI FIRMA GRAFOMETRICA

4.1 Ambito di utilizzo

Lo scenario di utilizzo del processo di Firma Grafometrica adottato da **Zanesi S.r.l.** prevede la digitalizzazione delle pratiche CONSENSO INFORMATO, ANAMNESI, MODULO ADESIONE SERVIZIO FEA, PRIVACY, PREVENTIVI. La soluzione adottata, prevede che la firma venga apposta su una tavoletta grafometrica collegata ad un PC desktop e che il formato dei documenti informatici sia di tipo PDF e/o PDF/A.

Non è escluso che il servizio di Firma Grafometrica possa essere esteso ad altri ambiti/servizi erogati da **Zanesi S.r.l.** per i propri utenti.

4.2 Ruoli Funzionali

Di seguito si riportano gli attori coinvolti nel servizio di Firma Grafometrica:

- **Firmatario:** i cittadini e relativi fiduciari che provvederanno ad apporre la propria firma sul documento informatico.
- **Operatore:** sono gli utenti definiti da **Zanesi S.r.l.** al riconoscimento certo degli utenti e provvederanno a controfirmare, apponendo la propria firma digitale sul documento informatico, precedentemente firmato dagli utenti.

4.3 Identificazione del/i Firmatario/i ed adesione al Servizio di Firma Grafometrica

Prima di raccogliere l'adesione/consenso dell'utente al servizio di Firma Grafometrica, l'Operatore identifica in modo certo il firmatario attraverso un documento di identità originale in corso di validità.

Una volta appurata l'identità, il firmatario prende visione dell'informativa del servizio erogato e comunica oralmente la volontà di aderire al servizio all'Operatore, il quale la raccoglie in un documento informatico che sottoscrive con la propria firma digitale.

Viene acquisita anche una copia digitale del documento d'identità del firmatario, che verrà aggregata al documento informatico di consenso.

Al termine del processo, il documento aggregato, contenente il documento informatico di adesione/consenso al servizio e la copia digitale del documento di identità dell'utente vengono inviati al sistema di conservazione digitale Docfly fornito da Aruba PEC, dove rimane a disposizione per eventuali successive consultazioni e/o copie per venti anni.

Copia dell'adesione/consenso può essere richiesta dall'utente in qualunque momento inviando una richiesta via e-mail all'indirizzo **info@zanesi.it** con oggetto "*Richiesta copia del consenso all'utilizzo del servizio di Firma Grafometrica*" con allegato la copia del documento d'identità del richiedente.



Allo stesso modo, il consenso può essere revocato in qualunque momento inviando una e-mail all'indirizzo **info@zanesi.it** con oggetto *“Richiesta revoca consenso servizio di Firma Grafometrica”* con allegato la copia del documento d'identità del richiedente.

I documenti richiesti saranno forniti via e-mail o con stampa cartacea.

Nel caso in cui il cittadino non intenda utilizzare il servizio di Firma Grafometrica si procederà con la predisposizione del documento in forma cartacea e con l'apposizione della firma autografa sul documento cartaceo.

4.4 Processo di sottoscrizione del documento informatico

Su ogni PC del soggetto erogatore viene collegata tramite interfaccia USB una tavoletta grafica digitale (Wacom modello STU-530) completa di software dedicato e certificato per la firma e relativa cattura e gestione dei dati grafometrici (AGI-Client di Aruba PEC S.p.A.).

I documenti da firmare sono in formato PDF, appositamente predisposti con i campi firma sia per il cittadino e relativi fiduciari, sia per l'Operatore.

Il firmatario, in presenza dell'Operatore che predispose il documento informatico con i dati relativi al cittadino e fiduciari, verifica il documento da firmare in ogni sua parte. Completata tale verifica appone la firma grafometrica su tavoletta grafica con un gesto naturale del tutto simile alla firma autografa.

Al termine di questo processo l'Operatore provvede a controfirmare con la propria firma digitale il documento informatico.

Al termine del processo di sottoscrizione il documento informatico non è più modificabile e ne viene garantita l'integrità e la leggibilità nel tempo.

All'interno del documento sono custoditi in modo sicuro tutti gli elementi necessari per eventuali e successive verifiche di perizia grafometrica in caso di contenzioso. Il PDF firmato con firma grafometrica è conforme allo standard PAdES.

Contestualmente, una volta che tutti gli attori hanno apposto le proprie firme sul documento informatico, l'Operatore provvede, su richiesta, a rilasciare al cittadino una copia conforme del documento sottoscritto, ed inviare lo stesso in Conservazione sostitutiva a norma.

4.4.1 Flusso Operativo

Di seguito viene riportato in dettaglio il workflow del processo di Firma Grafometrica:

Fase	Descrizione
1	L'utente si presenta dinanzi all'Operatore di Zanesi S.r.l. per eseguire un'operazione che richiede la Firma Grafometrica.
2	L'Operatore identifica in modo certo (DE-VISU) il firmatario e procede con la predisposizione del documento informatico.

Fase	Descrizione
3	L'Operatore informa il firmatario (se non ha mai utilizzato la Firma Grafometrica) della possibilità di utilizzare il servizio di Firma Grafometrica, fornendone termini e condizioni. In caso positivo provvede a raccogliere copia del documento d'identità del firmatario ed alla predisposizione del documento informatico da sottoscrivere.
4	L'immagine del documento informatico che deve essere sottoscritto con Firma Grafometrica, generato a conclusione dell'operazione, (o i suoi dati essenziali) sono visualizzati dal firmatario sullo schermo del PC.
5	L'Operatore evidenzia il punto di firma, quindi il firmatario procede apponendo la firma sulla tavoletta mediante apposita penna. Sullo schermo del PC è visualizzato il documento comprensivo dell'immagine della firma. Il firmatario verifica visivamente l'inserimento della propria firma sul documento nei punti indicati, e ne conferma l'apposizione. Eventualmente può annullare e ripetere il processo.
6	A conferma avvenuta la tavoletta acquisisce l'immagine della firma ed i dati biometrici ad essa associati. L'abbinamento dei dati genera una Firma Grafometrica non riproducibile da persona diversa dal firmatario.
7	La tavoletta, man mano che acquisisce i dati, li protegge con cifratura e li inoltra al PC.
8	L'applicazione decifra i dati biometrici ricevuti, i quali vengono poi legati indissolubilmente all'impronta informatica (hash) del documento. L'intero pacchetto (dati biometrici ed hash) è infine protetto con la chiave pubblica di cifratura nota al software di postazione (client), al fine di impedirne il successivo uso fraudolento
9	Il documento (arricchito con il pacchetto cifrato contenente i dati biometrici e l'hash) viene poi ulteriormente protetto con l'apposizione della firma digitale associata alla postazione, al fine di garantirne l'integrità. Il documento così ottenuto può essere successivamente modificato per la sola aggiunta di altre Firme Grafometriche. Ogni altra modifica differente dall'aggiunta di Firma Grafometrica causa l'invalidità del documento. Un'eventuale manomissione in questi termini verrebbe difatti rilevata facilmente, anche solo con la semplice lettura del documento tramite Adobe Reader
10	L'Operatore provvede a controfirmare il documento apponendo la propria firma digitale.
11	Qualora il firmatario lo richieda l'Operatore, grazie alle funzionalità fornite dalla libreria AGI, può anche provvedere alla stampa e consegna di una copia cartacea del documento, ove è visibile l'immagine della firma precedentemente apposta sulla tavoletta. In alternativa, è possibile estrarre copia elettronica (copia conforme) ed inviarla via e-mail.
12	Il documento informatico firmato è pronto per essere assoggettato al processo di protocollazione e conservazione come un qualunque altro documento avente firma elettronica.

Tabella 3: Processo di Firma

5 CARATTERISTICHE DEL SERVIZIO E DELLE TECNOLOGIE UTILIZZATE

Nel seguente capitolo si riportano le componenti e gli standard biometrici adottati per la realizzazione del servizio di Firma Grafometrica, adottato dal **Zanesi S.r.l.**

5.1 *Applicazione Client Desktop stand-alone*

Si tratta dell'applicazione **AGI Client** che provvede in autonomia ed in locale alla formazione del documento firmato grafometricamente.

L'applicazione interagisce con la specifica tavoletta grafica per l'acquisizione dei vettori grafometrici e dell'aspetto grafico della firma stessa, che provvederà ad utilizzare per portare a termine il processo di firma grafometrica.

Successivamente l'applicazione richiederà l'apposizione della Firma Digitale (a completamento della operazione di firma grafometrica) da parte dell'Operatore che presenzia l'atto di apposizione della firma grafometrica.

5.2 *Protezione dei dati Biometrici*

Il software **AGI CLIENT** pone particolare attenzione soprattutto all'aspetto della sicurezza in modo da:

- Garantire in ogni fase del processo, e in ogni componente logica, la riservatezza dei dati grafometrici dell'utente;
- Evitare che la firma apposta su un determinato documento possa essere riutilizzata in un documento differente;
- Rispettare tutti i vincoli normativi affinché la soluzione sia utilizzabile all'interno di un processo di FEA (Firma Elettronica Avanzata).

Nel contempo non sono ovviamente trascurati gli aspetti legati alla semplicità e all'intuitività del software con l'intento di fornire una soluzione che offra procedure snelle in grado di ricalcare quanto più è possibile la "user experience" di una normale firma autografa apposta su foglio di carta.

I dati biometrici della firma sono inseriti nel documento in forma cifrata mediante crittografia asimmetrica RSA almeno a 2048 bit, usando una chiave specificamente dedicata a tale operazione.

La chiave privata di decifratura (cui corrisponde la chiave pubblica indicata al punto precedente) viene custodita da una terza parte fidata, nel caso specifica presso la Certification Authority Aruba PEC, e non è normalmente acceduta da nessuno (custodita in modalità "off-line") tranne che dalle Autorità in caso di contenzioso.



I dati che vengono cifrati ed inseriti nel documento includono non solo i parametri biometrici della firma ma anche l'impronta (hash) del documento stesso.

Dopo l'apposizione delle necessarie firme grafometriche (una o più), il documento viene "sigillato" mediante una Firma Digitale.

5.3 Tablet/PAD Manager – Standard Biometrici utilizzati

Il modulo Tablet/PAD Manager è il componente software che ha il principale compito di disaccoppiare l'utilizzo di differenti dispositivi di acquisizione grafica (signature Pad o Tablet) dalle funzionalità core dei client.

Considerando infatti che ogni tipologia di tavoletta restituisce i vettori grafometrici in modo differente, il Tablet/PAD Manager si preoccupa di normalizzare le grandezze biometriche acquisite oltre che di indicare il modello della tavoletta grafica utilizzata così da inserirlo nelle informazioni riportate nella struttura dati di output.

Il Tablet/PAD Manager quindi normalizza l'output di ciascun dispositivo di acquisizione grafometrica già integrate nella soluzione consentendo una gestione univoca e standard dei vettori grafometrici acquisiti.

In particolare il Tablet/PAD Manager dopo la ricezione dei vettori grafometrici dal particolare dispositivo procede alla loro normalizzazione costruendo una struttura binaria conforme all'**ISO/IEC 19794-7:2014 FULL-FORMAT**.

L'unico vincolo per verificare l'autenticità di una Firma Grafometrica è rappresentato dalla compatibilità con il formato ISO/IEC 19794-7:2014 FULL-FORMAT.

Questo aspetto è di fondamentale importanza anche in virtù del fatto che il trattamento ISO dei vettori grafometrici consente la possibilità di importazione dei dati in strumenti di analisi forense di terze parti e la possibilità di eseguire efficacemente la perizia anche a distanza di anni dalla generazione della firma scongiurando il rischio che lo strumento originariamente previsto risulti inefficace.

Grazie all'estrema precisione dei dispositivi utilizzati (generalmente 200 point/sec), il Tablet/PAD Manager è anche in grado di acquisire un'immagine della firma autografa ad altissima risoluzione.

In aggiunta alla normalizzazione delle grandezze biometriche è necessario ricordare anche le esigenze legate alla **protezione, trattamento** e di **riservatezza** dei vettori.

In tal senso il Tablet/PAD Manager gestisce le transazioni di acquisizione in modo tale che nessun componente software o hardware coinvolto memorizzi mai i vettori grafometrici. Nel caso di utilizzo e gestione di tali dati, questi vengono gestiti sempre in maniera cifrata e, terminata la specifica operazione, vengono cancellati dalla memoria del dispositivo in uso.

Per raggiungere tale obiettivo il Tablet/PAD Manager istruisce il dispositivo di acquisizione affinché il canale di comunicazione tra il dispositivo ed il middleware sia cifrato con una chiave simmetrica AES-256 generata "on fly" per ogni sessione. Tale chiave viene negoziata attraverso uno schema di key-exchange basato su chiave RSA a 2048 bit. In aggiunta, a garanzia di una sicura acquisizione e gestione delle grandezze biometriche, il dispositivo di acquisizione viene gestito dal Tablet/PAD Manager in modo tale da garantire che l'invio dei dati avvenga per lotti, (il lotto ricevuto sarà decifrato e scritto nella struttura dati ISO) e che siano garantite le caratteristiche di Real time signature capture per evitare qualsiasi tipo di memorizzazione delle grandezze biometriche all'interno della memoria del dispositivo.



5.4 PDF Manager e gestione PDF

Il componente PDF Manager prepone alla creazione, gestione, predisposizione, elaborazione, visualizzazione e validazione dei file PDF e PDF/A.

Il PDF Manager è anche il componente che prepone all'innesto dei vettori grafometrici all'interno del documento realizzando, nel concreto, il file PDF/A finale con firma grafometrica.

5.5 GESTIONE DELLE LICENZE DELLE COMPONENTI SOFTWARE

Il modulo di licensing dell'applicazione AGI ha il duplice scopo di:

- Evitare che la libreria possa essere utilizzata su dispositivi non abilitati e/o in modalità non autorizzate;
- Gestire l'inizializzazione di tutte le quantità di sicurezza necessarie per la corretta predisposizione del Security Enviroment della libreria AGI;

6 Requisiti normativi

Di seguito si riportano gli obblighi previsti dalla normativa per il soggetto che eroga il servizio di Firma Elettronica Avanzata in modalità grafometrica:

Art. 57 comma 1 del DPCM 22/02/2013	Note
<p>a) Identificare in modo certo l'utente tramite un valido documento di riconoscimento, informarlo in merito agli esatti termini e condizioni relative all'utilizzo del servizio, compresa ogni eventuale limitazione dell'uso, subordinare l'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente.</p>	<p>Il firmatario viene riconosciuto ed informato direttamente presso l'apposito sportello del Zanesi S.r.l. da un Operatore addetto al servizio. La dichiarazione di accettazione/consenso viene fornita oralmente all'Operatore il quale la riporta in un documento informatico, contenente anche la copia digitale del documento di riconoscimento del firmatario, che successivamente provvede a firmare con la propria firma digitale. Il documento informatico firmato digitalmente viene poi protocollato ed inviato in Conservazione sostitutiva a norma.</p>
<p>b) Conservare per almeno venti anni la copia del documento di riconoscimento, la dichiarazione di cui alla lettera a) ed ogni altra informazione atta a dimostrare l'ottemperanza a quanto previsto dall'Art. 56 comma 1, garantendo la disponibilità, integrità leggibilità ed autenticità.</p>	<p>Il modulo digitale è conservato nel sistema di Conservazione sostitutiva a norma Docfly.</p>
<p>c) Fornire liberamente e gratuitamente copia della dichiarazione e le informazioni di cui alla lettera b) al firmatario, su richiesta di questo.</p>	<p>Richiedibile gratuitamente inviando richiesta via e-mail all'indirizzo: info@zanesi.it</p>
<p>d) Rendere note le modalità con cui effettuare la richiesta di cui al punto c), pubblicandole anche sul proprio sito internet.</p>	<p>Pubblicate sul sito istituzionale Zanesi S.r.l.: https://www.zanesi.it/fea</p>
<p>e) Rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dall'Art. 56 comma 1.</p>	<p>Pubblicate sul sito istituzionale Zanesi S.r.l.: https://www.zanesi.it/fea</p>
<p>f) Specificare le caratteristiche tecnologiche utilizzate e come queste consentano di ottemperare a quanto prescritto.</p>	<p>Pubblicate sul sito istituzionale Zanesi S.r.l. all'indirizzo: https://www.zanesi.it/fea</p>
<p>g) Pubblicare le caratteristiche di cui alle lettere e) ed f) sul proprio sito internet.</p>	<p>Pubblicate sul sito istituzionale Zanesi S.r.l. all'indirizzo: https://www.zanesi.it/fea</p>

Art. 57 comma 1 del DPCM 22/02/2013	Note
<p>h) Assicurare, ove possibile, la disponibilità di un servizio di revoca del consenso all'utilizzo della soluzione di Firma Elettronica Avanzata ed un servizio di assistenza.</p>	<p>Richiedibile gratuitamente inviando richiesta via e-mail all'indirizzo: info@zanesi.it</p>
Art. 57 comma 2 del DPCM 22/02/2013	Note
<p>Al fine di proteggere i titolari della firma elettronica avanzata e i soggetti terzi da eventuali danni cagionati da inadeguate soluzioni tecniche, i soggetti che erogano o realizzano soluzioni di firma elettronica avanzata si dotano di una copertura assicurativa per la responsabilità civile rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali per un ammontare non inferiore ad euro cinquecentomila.</p>	<p>POLIZZA N.HCC20-WM007716 DEL 14/12/2020</p>
Art. 58 del DPCM 22/02/2013	Note
<p>I soggetti che offrono una soluzione di firma elettronica avanzata alle Pubbliche Amministrazioni, devono essere in possesso della certificazione di conformità del proprio sistema di gestione per la sicurezza delle informazioni ad essi relativi.</p>	<p>Aruba PEC è prestatore di servizi fiduciari qualificati per emissione di validazione temporale e autorità di certificazione, identificazione digitale (SPID), servizi di conservazione a norma ed è presente nelle relative liste pubblicate da AgID a secondo quanto previsto nel Regolamento UE 910/2014 (c.d. "Regolamento eIDAS").</p> <p>Certificazioni in possesso di Aruba PEC S.p.A.</p> <ul style="list-style-type: none"> • Autorità di Certificazione accreditato presso AgID ed autorizzato all'emissione di certificati qualificati conformi alla direttiva europea ed italiana, certificati CNS, Marche Temporali ed Identità Digitali (SPID). • Gestore di Posta Elettronica Certificata dal 12/10/2006, accreditato presso AgID ed autorizzato alla gestione di caselle e domini di Posta Elettronica Certificata (PEC) • Certificata UNI EN ISO 9001:2015 • Certificata ISO/IEC 27001:2013 <p>Maggiori dettagli sulle certificazioni di Aruba PEC sono disponibili all'indirizzo: https://www.aruba.it/certificazioni.aspx</p>

Tabella 4: Requisiti Normativi