



Istituto Comprensivo Statale "Valle dell'Anapo" - Ferla (Siracusa)

Via Pessina, snc. – 96010 Ferla (SR)



Ferla 09 Marzo 2018

FIRMA GRAFOMETRICA (Firma Elettronica Avanzata – FEA)

Normativa di riferimento

L'Istituto Comprensivo Statale "Valle dell'Anapo" di Ferla (SR), nell'ambito dello sviluppo di processi innovativi volti a ridurre l'uso della carta e aumentare l'efficienza dei processi, ha scelto di mettere a disposizione dei propri utenti ed operatori un servizio di Firma Elettronica Avanzata, basato su Grafometria ai sensi del D.Lgs. 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale", in ottemperanza al DPCM 22 febbraio 2013 recante "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, e 71.?" ed al Provvedimento generale prescrittivo in tema di biometria " 12 novembre 2014 n. 513 del Garante per la protezione dei dati personali.

Le soluzioni tecnologiche adottate consentono di sostituire i documenti cartacei con cosiddetti documenti informatici, in grado di rendere più veloce l'operazione di raccolta della sottoscrizione, garantendo la medesima validità ed efficacia probatoria dei tradizionali documenti cartacei, ai sensi degli Articoli 2702 e 1350, comma 1, numero 13 del Codice Civile. Inoltre, l'utilizzo di tali sistemi, da un lato, si giustifica al fine di contrastare eventuali tentativi di frodi e il fenomeno dei furti di identità e, dall'altro, ha lo scopo di rafforzare le garanzie di autenticità e integrità dei documenti informatici sottoscritti, anche in vista di eventuale contenzioso legato al disconoscimento della sottoscrizione apposta, sia su atti e documenti

DF\sa





REGIONE SICILIA



Unione Europea

FONDI
STRUTTURALI
EUROPEI



2014-2020

PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO (FSE-FESR)



MIUR



Istituto Comprensivo Statale "Valle dell'Anapo" - Ferla (Siracusa)

Via Pessina, snc. – 96010 Ferla (SR)

interni che su istanze raccolta dagli utenti.

La Scuola, consapevole della possibilità di cui al punto precedente, ha scelto di adottare, nei rapporti con i propri utenti, un particolare servizio di elaborazione e sottoscrizione dei documenti con Firma Elettronica Avanzata (in breve "FEA" oppure ("Firma Grafometrica"), di seguito denominato "Servizio", che consente di apporre la propria firma utilizzando uno speciale tablet ed una penna elettronica; si tratta di sistemi di firma grafometrica posti a base di una soluzione di firma elettronica avanzata, così come definita dal D.Lgs. 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale" che non prevedono la conservazione centralizzata di dati biometrici.

L'operazione di apposizione della Firma Elettronica Avanzata da parte del Utente, caratterizzata da semplicità e immediatezza, permette di registrare ed elaborare, all'interno del documento informatico, oltre al tratto grafico della firma, una serie di dati comportamentali propri del Utente nell'atto della sottoscrizione, quali la velocità, la pressione esercitata, l'accelerazione dei movimenti, nonché i movimenti effettuati dalla penna quando è sollevata dal tablet (salti in volo); essi assumono il valore di dati biometrici.

Il Servizio proposto garantisce il rispetto dei requisiti di legge ed in particolare, l'identificazione del firmatario, la connessione univoca della firma, nonché della firma al documento sottoscritto ed il controllo esclusivo del sistema di generazione della firma in capo al firmatario medesimo; le caratteristiche tecniche della soluzione, inoltre, garantiscono l'integrità del documento in termini di immutabilità ed inalterabilità del suo contenuto (Art. 56 delle Regole Tecniche - DPCM 22 febbraio 2013).

Caratteristiche del sistema

La descrizione riportata di seguito è nel rispetto degli obblighi indicati alla lettera e) dell'Art. 57 del DPCM 22.02.2013 (*rendere note le caratteristiche del sistema realizzato atte a garantire quanto prescritto dall'art. 56, comma 1*).

a) *L'identificazione del firmatario del documento;*

Al fine dell'identificazione, gli Operatori della Scuola richiedono al firmatario un documento di riconoscimento in corso di validità.

Il tratto grafico unitamente ai dati biometrici, rilevati con adeguata precisione, dal tablet all'atto della firma, sono propri ed identificativi del soggetto che l'appone.

b) *La connessione univoca della firma al firmatario;*

E' soddisfatta dal tablet e dal Software di Firma che garantiscono:

- la connessione univoca tra dispositivo di firma ed il Software di Firma,
- il legame tra HASH del documento e la firma dell'Utente,

DF\sa



Unione Europea

FONDI
STRUTTURALI
EUROPEI

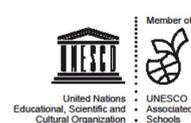


2014-2020

PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO (FSE-FESR)



MIUR



Istituto Comprensivo Statale "Valle dell'Anapo" - Ferla (Siracusa)

Via Pessina, snc. – 96010 Ferla (SR)

- c) *Il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;*
Il firmatario ha il controllo esclusivo del sistema di generazione della firma, avendo sempre la possibilità per ogni singola firma apposta, sul documento, di:
- Visualizzare il documento in modo da aver evidenza di quanto da lui sarà sottoscritto,
 - Apporre la firma sul documento,
 - Confermare la firma apposta,
 - Cancellare la firma apposta e ripetere la firma,
 - Annullare l'operazione di firma.
- d) *la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;*
- Il firmatario ha sempre la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma; presso AgID all' URL <http://www.agid.gov.it/identita-digitali/firme-elettroniche/software-verifica> sono disponibili, gratuitamente, una serie di software conformi alla [CNIPA DEL.45]. Anche Adobe Acrobat Reader® è in grado di eseguire la verifica.
- e) *la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;*
- Il firmatario ha sempre evidenza di quanto sottoscrive perché sul dispositivo è visualizzato il documento, inoltre potrà richiedere la stampa del documento originale, o l'invio dello stesso per e-mail o PEC.
- f) *L'individuazione del soggetto di cui all'art. 55, comma 2, lettera a), La Scuola;*
- Il firmatario è sempre in grado di identificare con certezza la Scuola (il soggetto che eroga la soluzione di firma) in quanto gli assistenti amministrativi della scuola lo informano con puntualità e chiarezza ed i loghi sono ben evidenziati
- g) *L'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;*
- E' garantita dalla tipologia dei documenti che sono tutti in formato PDF non modificabili e privi di qualsiasi funzione che possano nel tempo modificare il contenuto originale del documento.
- h) *La connessione univoca della firma al documento sottoscritto.*
- E' garantita dal Software di Firma che utilizzano algoritmo SHA per collegare il documento alla firma.

I requisiti sopra descritti soddisfano l'art. 56 delle Regole Tecniche [DPCM 22/02/2013] e l'Art. 21 comma 2-bis del CAD.

DF\sa



Istituto Comprensivo Statale “Valle dell’Anapo” - Ferla (Siracusa)

Via Pessina, snc. – 96010 Ferla (SR)

Caratteristiche delle tecnologie

La descrizione riportata di seguito è nel rispetto degli obblighi indicati alla lettera f) dell’Art. 57 del DPCM 22.02.2013 (specificare le caratteristiche delle tecnologie utilizzate e come queste consentono di ottemperare a quanto prescritto)

La Scuola I.C. “Valle dell’Anapo” e Namirial s.p.a. hanno prestato particolare attenzione alla sicurezza del dato biometrico acquisito. Mentre il firmatario esegue la firma, i dati biometrici che la caratterizzano sono immediatamente cifrati dal Client di firma con la chiave simmetrica AES, la cui chiave a sua volta è cifrata con la chiave pubblica dell’algoritmo asimmetrico RSA.

Il firmatario ha il controllo esclusivo del processo di firma, e dispone delle funzioni:

- di scorrere il documento in modo di aver evidenza di quanto da lui sarà sottoscritto,
- di firmare con la penna elettronica sul display del dispositivo di firma nell’apposita area di firma presentata in modo esplicito,
- con il tasto [Fine] si confermare la firma apposta,
- con il tasto [Riprova] si cancellare la firma apposta e si ripetere la firma,
- con il tasto [Annulla] si annullare l’operazione di firma.

Con la conferma da parte del firmatario della firma apposta, il Client di Firma immediatamente calcola l’impronta del documento informatico con l’algoritmo SHA.

I dati biometrici cifrati, la chiave AES cifrata, il tratto grafico ed altri dati, sono inseriti nel documento PDF.

Alla fine del processo il Client di Firma, firma il documento in standard PAdES, con un certificato di firma qualificato, secondo la deliberazione CNIPA 21 maggio 2009, n.45 [CNIPA Del.45].

Quest’ultima firma garantisce l’integrità (documento non alterato) e autenticità del documento informatico.

Il sistema descritto da una parte acquisisce dati personali comportamentali, riconducibili alla biometria, dall’altra prevede che tali dati non siano nella disponibilità del soggetto che li detiene, dando un altissimo livello di sicurezza al processo di firma.

Chiavi e Certificati

La descrizione riportata di seguito è nel rispetto del Provvedimento generale prescrittivo in tema di biometria - 12 novembre 2014 n. 513 paragrafo 4.4 del Garante della protezione dei dati personali e del DPCM 22.02.2013.

CHIAVE PUBBLICA DI CIFRATURA

La chiave pubblica di cifratura è compilata con il Software di Firma ed è utilizzata dallo stesso per cifrare la chiave AES, che a sua volta è utilizzata per cifrare i dati biometrici ed altre informazioni utili al processo di firma.

Le chiavi pubblica e privata sono generate dalla Certification Authority Consiglio Nazionale del Notariato (S.C.N.N.) accreditata presso AgID.

DF\sa



Istituto Comprensivo Statale "Valle dell'Anapo" - Ferla (Siracusa)

Via Pessina, snc. – 96010 Ferla (SR)

CHIAVE PRIVATA DI CIFRATURA

La chiave privata di cifratura, l'unica in grado di estrarre in chiaro la chiave AES che a sua volta è utilizzata per decifrare i dati biometrici, è conservata da un ente terzo fiduciario: la Certification Authority Consiglio Nazionale del Notariato (S.C.N.N.).

L'ente terzo sarà chiamato dall'autorità giudiziaria in caso di contenzioso, e seguirà le modalità di consegna indicate dalla stessa.

In nessun caso la Scuola avrà disponibilità di tale chiave come pure il Utente.

CERTIFICATO DI FIRMA

Il certificato di firma digitale è utilizzato dal Client di Firma al termine del processo di Firma Elettronica Avanzata, per garantire l'integrità (documento non alterato) e autenticità (autore Technology Estate) del documento digitale.

Il Certificato è generato dalla Certification Authority In.Te.S.A. S.p.A. (An IBM Company) accreditata presso AgID.

Indennizzi

La Scuola, soggetto che eroga la soluzione di Firma Elettronica Avanzata, come indicato nelle Regole Tecniche [DPCM 22/02/2013] art. 57 comma 4, non è tenuto a stipulare una polizza assicurativa per responsabilità civile.

Privacy

L'adozione della firma grafometrica implica il trattamento dei dati biometrici.

La cifratura dei dati grafometrici è effettuata con le modalità descritte al paragrafo 15.2 del Manuale Operativo ed i dati non sono usufruibili né dalla Scuola, né dal firmatario.

Essendo la Scuola il Titolare del trattamento dei dati come indicato al comma 1 lettera a) dell'Art. 37 del DL 196/2003, la Scuola ha provveduto a notificare il trattamento con le modalità dell' Art. 38 del DL 196/2003.

Il Garante ha inserito nel registro dei trattamenti la notifica della Scuola.

La notifica è accessibile gratuitamente a chiunque per via telematica all'URL <http://www.garanteprivacy.it/>

Le notifiche accessibili tramite la consultazione del registro possono essere trattate per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali.

DF\sa