ISTITUTO ISTRUZIONE SECONDARIA SUPERIORE
DEL PRETE - FALCONE
SAVA

SETTORE TECNOLOGICO: TATF04101B
Biotecnologie Sanitarie - Elettronica ed Elettrotecnica
Informatica e Telecomunicazioni - Meccanica e Meccatronica
CORSO SERALE: TATF04151R *Elettronica ed Elettrotecnica*

LICEO SCIENTIFICO
TAPS041019
Scienze Applicate

SETTORE PROFESSIONALE: TARF04101G
Servizi Socio Sanitari – Produzioni Industriali e Artigianali
CORSO SERALE: TARF041511 *Servizi Socio Sanitari*
IPIA. San Marzano di S.G.:TARI04101E *Manutenzione e Assistenza Tecnica*
CORSO SERALE: TARI04151X *Manutenzione e Assistenza Tecnica*

CARATTERISTICHE DEL SISTEMA DI FIRMA ELETTRONICA AVANZATA

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).

1. 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 la appone.

2. La connessione univoca della firma al firmatario
   È soddisfatta dal tablet e dal Software di Firma che garantiscono:
   a. la connessione univoca tra dispositivo di firma ed il Software di Firma
   b. il legame tra HASH del documento e la firma dell'Utente

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
   Il firmatario ha il controllo esclusivo del sistema di generazione della firma, avendo sempre la possibilità per ogni singola firma apposta, sul documento, di:

   a. Visualizzare il documento in modo da aver evidenza di quanto da lui sarà sottoscritto
   b. Apporre la firma sul documento
   c. Confermare la firma apposta
   d. Cancellare la firma apposta e ripetere la firma
   e. Annullare l'operazione di firma

4. 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-ver..., sono disponibili, gratuitamente, una serie di software conformi alla [CNIPA DEL.45]
   Anche Adobe Acrobat Reader® è in grado di eseguire la verifica.

5. 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.

6. 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.

7. L’assenza di qualunque elemento nell’oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati
   È 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.

8. La connessione univoca della firma al documento sottoscritto
   È 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.

Indennizzi

L’Istituto, 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 la polizza assicurativa per responsabilità civile.

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).
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 [OK] si confermare la firma apposta
- con il tasto [CLEAR] 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.

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