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. di Castellucchio 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.