ing. Stefano Spiniello	32	
ing. Giuseppina Ventre	33	
geom. Nicodemo Zavaglia	34	

Nel lettore biometrico del terminale **NON** sono quindi presenti:

- Dati anagrafici dell'utente

- Immagine dell'impronta digitale dell'utente: l'immagine catturata è contestualmente elaborata dal processore ed **in nessun modo acquisita o conservata dal lettore biometrico** e quindi non è possibile in alcun modo ricavare tale immagine perché **inesistente**.

- Dati fisici diretti o deducibili dell'impronta digitale: il modello archiviato ottenuto mediante algoritmo è un numero senza alcun significato diretto o indiretto relativamente ai dati fisici dell'impronta digitale.

La "ricostruzione dell'impronta digitale" partendo dal modello non è possibile, nemmeno conoscendo l'algoritmo di elaborazione per definizione stessa di algoritmo matematico irreversibile.

Restando a disposizione per qualsiasi ulteriore richiesta o chiarimento si porgono distinti saluti.

Avv. Federica Spuri Nisi

Da "Posta Halley" <halleynt@halley.it>
A "mcimbimbo@enteidricocampano.it" <mcimbimbo@enteidricocampano.it>
Data mercoledì 19 giugno 2019 - 11:56

Prot. N.60928 del 19-06-2019 - Funzionamento terminali presenze con lettore di impronte digitali

Gentile Dott.ssa Imbimbo,
facendo seguito alla telefonata intercorsa ieri, con la presente sono a rappresentarLe il funzionamento dei terminali presenze acquistati dall'Ente Idrico Campano.

Il funzionamento del lettore di impronte digitali, quale strumento di verifica biometrica comprende 2 fasi principali:

A) **Registrazione** (enrolment): le caratteristiche dell'impronta digitale sono acquisite tramite il lettore del terminale, digitalizzate, elaborate e compresse mediante un algoritmo matematico irreversibile (da non confondersi con il processo di crittografia) fino ad ottenerne un modello matematico (*template*) che, associato al codice identificativo della persona, diviene la base dei successivi confronti o verifiche.

B) **Verifica** (matching): le caratteristiche dell'impronta digitale sono acquisite, digitalizzate, elaborate e compresse in modo identico a quello della fase di registrazione fino ad ottenere un analogo modello matematico. Il confronto tra il modello (*template*) archiviato relativo al codice di riferimento ed il risultato della lettura determina, in base allo scostamento, il risultato della verifica.

In sostanza ciò significa che i sensori biometrici per il riconoscimento delle impronte digitali sono dei veri e propri scanner che catturano un'immagine della caratteristica biometrica e attraverso algoritmi matematici UNIDIREZIONALI la convertono in punti a cui assegnano delle coordinate x/y.
L'algoritmo proprietario converte queste coordinate di punti in stringhe numeriche (Byte) che vengono memorizzate in un modello da utilizzare per i confronti successivi.
Nel modello (template) perciò **vengono memorizzati solo dei numeri** di riferimento delle coordinate x/y dei punti e **non** la caratteristica biometrica vera e propria. Questo rende impossibile risalire dal template all'impronta stessa, rendendo così sicura, in materia di privacy, l'identità dei soggetti registrati.
L'identità non può quindi essere clonata o riutilizzata, per il semplice fatto che **non è mai memorizzata**!
È molto importante, per ovvie ragioni, essere assolutamente certi circa l'impossibilità di estrarre dal codice numerico, creato dall'elaborazione delle chiavi biometriche, l'immagine della caratteristica somatica utilizzata per il riconoscimento; questa garanzia è data dalla non reversibilità del codice numerico creato con l'algoritmo unidirezionale.

DATI ARCHIVIATI

Dopo l'enrolment, il template viene memorizzato per poter essere in seguito confrontato (come spiegato in precedenza).
Il template è memorizzato sul badge in dotazione all'utente e vengono archiviati solo i seguenti dati :

- Codice utente: è un puro codice di riferimento, assimilabile al numero di matricola.

- Modello (template): è un puro numero, assimilabile al codice presente in una banda magnetica di un badge. Quando i template sono memorizzati sul badge dell'utente i confronti tra quello memorizzato e quello generato al momento vengono eseguiti sempre a livello locale senza lasciarli poi memorizzati sul terminale. Questa modalità garantisce ulteriormente l'utente sulla riservatezza del dato (il template è memorizzato SOLO sul badge in dotazione).

- Elenco Eventi: data/ora, codice utente, indirizzo del terminale ed eventuale codice causale (giustificativo) sono gli unici risultati memorizzati dopo le verifiche operate dal lettore biometrico, dati equivalenti ai dati "classici" di un terminale di gestione presenze.

ENTE IDRICO CAMPANO

Ai dipendenti dell'Ente Idrico Campano
LORO SEDI

OGGETTO: **Regolamento Generale sulla Protezione Dati (RGPD UE 2016/679).**
Informativa sulla privacy ai sensi dell'art. 13 e trattamento dati biometrici.
Trasmissione ai dipendenti dell'EIC.

Ai sensi dell'art. 13 del Regolamento Europeo per la Protezione dei Dati (RGPD UE 2016/679), l'Ente Idrico Campano, nella qualità di titolare del trattamento dei dati, con la presente nota, in appendice all'informativa già inviata ai dipendenti con nota prot. n. 2147 del 6/2/2019, informa tutti i lavoratori, che verranno trattati dati biometrici (in particolare l'impronta digitale) per la specifica finalità di rilevazione delle presenze in servizio.

In merito alle modalità di trattamento dei dati biometrici, si precisa che:

a) nella fase di registrazione del dato biometrico (o enrollment), lo stesso non sarà conservato in alcun database (se non per il tempo necessario all'elaborazione), ma acquisito tramite il lettore del terminale, digitalizzato, elaborato e compresso mediante un algoritmo matematico **irreversibile**, fino ad ottenerne un modello matematico (*template*) che, associato al codice identificativo della persona, diviene la base delle successive verifiche;

b) nella fase di verifica del dato biometrico (o matching), le caratteristiche dell'impronta digitale sono acquisite con le medesime modalità utilizzate nella fase di registrazione. Si ottiene pertanto anche in tale fase un modello matematico che, confrontato con il modello archiviato, determinerà, in base allo scostamento, il risultato della verifica.

In sostanza, i sensori biometrici per il riconoscimento delle impronte digitali catturano un'immagine della caratteristica biometrica e attraverso algoritmi matematici unidirezionali la convertono in punti, a cui assegnano delle coordinate x/y.

L'algoritmo proprietario converte queste coordinate di punti in stringhe numeriche che vengono memorizzate in un modello da utilizzare per i confronti successivi. Nel modello (template) perciò vengono memorizzati dei numeri di riferimento delle coordinate x/y dei punti e non la caratteristica biometrica vera e propria.

Non è pertanto possibile estrarre dal codice numerico, creato dall'elaborazione delle chiavi biometriche, l'immagine della caratteristica somatica utilizzata per il riconoscimento; tale garanzia è dovuta alla non reversibilità del codice numerico creato con l'algoritmo unidirezionale.

Quando i template sono memorizzati sul badge dell'utente, i confronti tra quello memorizzato e quello generato al momento, vengono eseguiti sempre a livello locale, senza lasciarli memorizzati sul terminale. Questa modalità garantisce ulteriormente l'utente sulla riservatezza del dato.
Il template è memorizzato sul badge in dotazione e vengono archiviati solo il codice utente, un numero assimilabile al numero di matricola; il template, modello matematico; l'elenco degli eventi: data/ora, codice utente, indirizzo del terminale ed eventuale codice causale (giustificativo).