# Le soluzioni biometriche di Kaba

*a cura della Redazione*

Il Garante per la Privacy ha approvato un quadro unitario di misure e accorgimenti di carattere tecnico, organizzativo e procedurale per mantenere alti livelli di sicurezza nell'utilizzo dei dati biometrici, semplificando tuttavia alcuni adempimenti. L' intervento del Garante si è reso necessario alla luce della crescente diffusione di dispositivi dotati di questa tecnologia.

Sempre più spesso, infatti aziende e pubbliche amministrazioni si servono di dati biometrici come, per esempio, le impronte digitali per il controllo degli accessi, per l'autenticazione degli utenti o per la sottoscrizione di documenti informativi.

Nel Provvedimento generale in tema di riconoscimento biometrico e firma grafometrica, il Garante ha individuato alcune tipologie di trattamento che, per le specifiche finalità perseguite, presentano un livello ridotto di rischio e non necessitano più della verifica preliminare da parte dell'Autorità, a condizione che vengano adottate tutte le misure e gli accorgimenti tecnici individuati nel provvedimento e vengano rispettati tutti i presupposti di legittimità previsti dal Codice Privacy.


*Lettore biometrico Kaba 91 50*

Le tipologie di trattamento dei dati biometrici considerati nel Provvedimento sono:

**Autenticazione informatica**

Le caratteristiche biometriche dell'impronta digitale o dell'emissione vocale di una persona possono essere utilizzate come credenziali di autenticazione per l'accesso a banche dati e sistemi informatici, anche senza il consenso dell'utente.

**Controllo di accesso fisico ad aree "sensibili" dei soggetti addetti e utilizzo di apparati e macchinari pericolosi**

Le caratteristiche dell'impronta digitale o della topografia della mano potranno essere trattate per consentire l'accesso ad aree e locali ritenuti "sensibili" oppure per consentire l'utilizzo di apparati o macchinari pericolosi, anche senza il consenso degli utenti.

**Sottoscrizioni dei documenti informatici**
L'analisi dei dati biometrici associati all'apposizione a mano libera di una firma autografa potrà essere utilizzata per la firma elettronica avanzata, solo con consenso utenti.

**Scopi facilitativi**
L'impronta digitale e la topografia della mano potranno essere utilizzati anche per consentire l'accesso fisico di utenti ad aree fisiche in ambito pubblico (es. biblioteche) o privato (es. aree aeroportuali riservate), solo con consenso degli utenti.

Le soluzioni offerte da **Kaba** rispondono ai requisiti principali presenti nel nuovo documento del Garante, in quanto non prevedono alcun tipo di archiviazione centralizzata o distribuzione dei dati biometrici in rete. La soluzione di "verifica" **Kaba**, infatti, combina l'utilizzo del badge con l'impronta biometrica; le impronte infatti sono memorizzate direttamente sul media/badge e gestiti tramite i terminali **Kaba** sotto forma di template, quindi il dato biometrico è protetto attraverso tecniche crittografiche.


*Terminale Kaba B-web 97 00, versione con lettore biometrico*

Anche nella fase di acquisizione, il dato biometrico (enrollment) resta segreto e nascosto all'operatore.
Inoltre, le tecnologie di supporto sono media/badge compatibili con i livelli di sicurezza richiesti dal Garante, utilizzando chip tecnologicamente avanzati **Legic Advant ATC 4096**, **Mifare Desfire EV1** e, più in generale, i dispositivi che prevedono un livello di sicurezza minimo (Common Criteria) **CCEAL 4+**.
Tutti i terminali biometrici di ultima generazione **Kaba**, inoltre, sono da ritenersi sicuri grazie al sensore biometrico utilizzato **Morpho Smart CBM-E** di alta qualità e certificato dall'FBI con standard di riferimento equivalente ISO 19794-4:2011. I dispositivi **Kaba** hanno quindi la capacità di rilevare la vividezza dell'impronta, come specificato dai requisiti del Garante.
La soluzione è in grado, infine, di gestire anche progetti che prevedono l'utilizzo della tecnologia biometrica in modalità di "identificazione" , cioè con l'uso di soli template registrati su basi dati e non più con l'utilizzo del badge. In tal caso, le regole da seguire sono molto restrittive e coinvolgono tutto il sistema cliente dalla rete dati, che deve essere crittografata, alla base dati che deve risiedere in un ambiente estremamente protetto. Di conseguenza, i progetti in modalità "identificazione" richiedono una stretta collaborazione con il cliente, che diventa il player principale nella gestione del dato biometrico (registrazione e distribuzione).

KABA®
BEYOND SECURITY

CONTATTI: KABA SRL
info.it@kaba.com
www.kaba.it