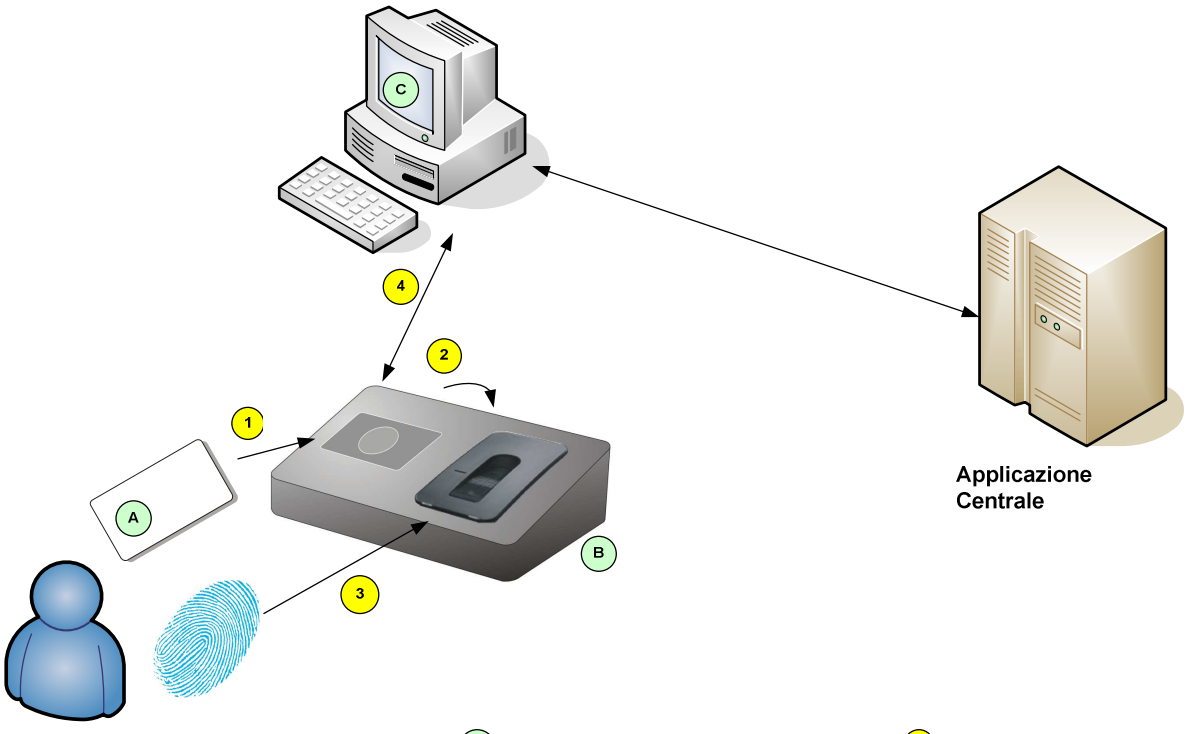
Soluzioni ad impronta digitale
Il N. 1 in Europa

SISTEMA PER
"AUTENTICAZIONE BIOMETRICA"

Schema di funzionamento

Il prodotto proposto è un sistema di autenticazione perché non individua un utente ma controlla solamente la corrispondenza tra le credenziali e i dati biometrici provvisti dall'utente stesso.



A Smartcard

B Device biometrico
Con capacità elaborativa autonoma

C Applicativo ad accesso controllato

1 Smartcard fornita dall'utente

2 Caricamento temporaneo
del template per il confronto

3 Confronto con lettura impronta

4 Comunicazione crittografata dell
autenticazione utente all'applicativo

ekey biometric systems Srl Via del Vigneto 35/A/Weinbergweg 39100 Bolzano/Bozen (BZ) http:www.ekey.net
Mail: italia@ekey.net Tel.: 0471 922712 Fax: 0471 508662

Operatività:

Per spiegare la funzionalità del sistema il sistema più semplice è quello di analizzare l'operatività:

1. L'utente pone la smartcard sul lettore, il sistema preleva tre informazioni dalla stessa:

   - Credenziali utente
   - Template biometrica dell'impronta
   - Codice di controllo

   L'accesso alla memoria della scheda è vincolata da una chiave crittografica basata sullo standard AES adottato a livello governativo dagli Stati Uniti d'America per la protezione dei documenti riservati.

2. I dati vengono verificati per la corrispondenza tra credenziali,e template e codice di controllo, in caso positivo il template viene copiato nel sotto-sistema di validazione biometrica per il confronto.

3. L'utente striscia il dito sul sensore termico, il sotto-sistema biometrico confronta le minuzie selezionate confrontandole con il template comunicando al sistema di controllo il risultato.

4. Il sistema di controllo verifica in continuo la situazione cancellando il template biometrico in ogni caso passato il tempo massimo (solitamente 6 secondi).
   In caso di verifica corretta biometrica il sistema di controllo comunica in modo crittografato i dati al computer, limitatamente alle credenziali e un codice di controllo temporale.

I passi Seguiti nel caso di autenticazione alternativa (disponibile per legge) avviene con la sostituzione del PIN al dato biometrico e rispettando i medesimi passi con la differenza che il PIN stesso viene fornito dal PC.

Composizione Hardware:

Il device biometrico si compone dei seguenti sotto-sistemi:

- Sistema di controllo
- Lettore di smart card
- Sensore biometrico con capacità elaborativa

Il device biometrico è dotato di alimentazione autonoma e comunica con il PC, che ospita l'applicazione sotto controllo, tramite connessione di rete Ethernet e protocollo TCP/IP.
Il sistema di controllo governa i sotto-sistemi permettendo un operatività completamente autonoma ad esclusione della mera comunicazione delle credenziali in caso di autentica e della ricezione delle stesse in caso di registrazione di una nuova smart card.

Sicurezza:

Per ragioni di sicurezza il device si caratterizza per:

- Non far uscire in nessun caso i dati biometrici sulla connessione verso il PC
- Avere capacità elaborativa autonoma, la comunicazione verso il PC è limitata alla comunicazione dell'autentica delle credenziali
- Usare un sistema di codifica dei dati a doppia chiave che non permette al produttore di software e al gestore dell'impianto di estrarre i dati dalle smart card
- Usare come algoritmo di memorizzazione dei dati sulla smart card e nelle comunicazioni con il PC l'algoritmo AES a 128 bit, standard di massima sicurezza riconosciuto
- Usare come dato biometrico un template che non permette in nessun caso di risalire all'impronta originale
- Memorizzare tutti i dati sulla smart carta crittografati, nessuno è in chiaro
- Fare in modo che il tempo di conservazione del template per il confronto è di pochi secondi scaduti i quali il template biometrico viene cancellato.
- Usare un sotto-sistema biometrico dotato di un sensore termico che garantisce la massima sicurezza e l'impossibilità di carpire l'impronta dell'ultima lettura effettuata dalla superficie del sensore stesso
- Non usare archivi di dati biometrici ne centralizzati e tanto meno sul device stesso, l'unico dato biometrico presente è quello letto dalla smart card per il tempo ristretto della verifica

A livello organizzativo inoltre si qualifica per:

- Il supporto dei dati biometrici, la smart card, rimane nell'esclusiva disponibilità del proprietario degli stessi
- La smart card è anonima, completamente bianca, non riportando dati identificativi del proprietario o dell'uso della stessa

Registrazioni Utenti (Smart card):

La registrazione degli utenti avviene da una postazione specifica, il device è dello stesso tipo.

La fase di registrazione viene effettuata con i seguenti passi:

1. L'operatore identifica l'utente come da specifiche organizzative e comunica, tramite specifico software, le credenziali con il comando di registrazione dell'utente al device biometrico

2. Il sistema di controllo abilita il sotto-sistema biometrico per la lettura dell'impronta e l'estrazione del template

3. L'utente striscia il dito sul sensore termico

4. Il sotto-sistema comunica l'estrazione dei dati e la preparazione del template al sistema di controllo

5. Il sistema di controllo crittogragrafa i seguenti dati:

   - Credenziali utente
   - Template
   - Codice di controllo

6. Il blocco di memoria viene memorizzato sulla smart card e la memoria del device viene ripulita di ogni riferimento

Alternativa secondo normativa senza credenziali biometriche:

Nel caso di smart card senza dati biometrici (autenticazione alternativa come da normativa) viene messo sulla stessa un Pin temporaneo che l'utente dovrà in seguito autonomamente aggiornare.

Soluzioni ad impronta digitale
Il N. 1 in Europa

Riferimenti alla normativa sulla privacy

(A) *Il sistema si qualifica come un sistema di autenticazione perché confronta il singolo dato biometrico fornito dall'utente con le credenziali e il codice di controllo fornite dallo stesso.*

Usando come riferimento il documento "Documento di lavoro sulla biometria" del 1.8.2003 redatto dal GRUPPO PER LA TUTELA DEI DATI PERSONALI citato come fonte nelle comunicazioni del garante possiamo trovare la seguente definizione:
"L'autenticazione risponde alla domanda: sono la persona che dichiaro di essere? Il sistema certifica l'identità della persona grazie all'elaborazione di dati biometrici che si riferiscono all'individuo autore della domanda e prende una decisione sì/no (confronto 1:1). L'identificazione risponde alla domanda: chi sono io? Il sistema riconosce l'individuo autore della domanda distinguendolo da altre persone i cui dati biometrici sono a loro volta registrati. In questo caso il sistema prende una decisione "1 su n" e risponde che la persona che pone la domanda è X."

Il sistema fa esclusivamente un confronto 1:1 e in nessun caso opera su una base dati con più dati biometrici, locale o remota. Quindi l'unica operatività permessa è quella di autenticazione con i dati forniti sulla smart card e in nessun caso di identificazione.

(B) *Il sistema costituisce una misura minima di sicurezza come specificato nell'art. 34, comma 1, lett. a del codice sulla privacy, in particolare a quanto previsto dall'allegato tecnico che individua le caratteristiche biometriche come sistema previsto di autenticazione informatica*.

(C) Il sistema è conforme al decalogo esplicitato dal Garante nel Comunicato Stampa del 9 maggio 2006, in particolare:

1. Affidabilità del sistema di rilevazione dei dati corporei.
   Il sistema usa un sensore biometrico diffusamente utilizzato in Europa dalle comprovate caratteristiche tecniche con rate di riconoscimento di 1 su 1milione. Il sistema è stato soggetto a diverse verifiche tecniche indipendenti che sono disponibili in allegato.
2. Informativa chiara, lasciando comunque la libertà di aderire o meno al sistema, salvo stringenti ragioni, indicando nella stessa informativa espressamente le tecniche alternative all'utilizzo dei dati corporei.
   Vedi l'informativa in allegato, per gli utenti che non aderiscono alle modalità biometriche è possibile utilizzare una smart card dotata di credenziali che viene abilitata tramine PIN.
   Le modalità operative sono le medesime, l'unica differenza risiede nella fornitura del PIN in sostituzione del dato biometrico
3. Liceità verificabile indubitabilmente sotto i profili di necessità, proporzionalità, finalità, correttezza, adeguatezza e qualità dei dati, previa acclarata dimostrazione dell'inefficacia di pratiche alternative che abbiano meno rischi di profilabili abusi. In particolare, qualora l'uso dei dati corporei sia permesso, deve essere comunque il più possibile circoscritto (ad esempio impronta di un dito invece di più dita).
   Per la necessità e proporzionalità, finalità si fa riferimentoa quanto riportato nel capitolo "Sensibilità del database e problematiche di sicurezza".
   Per l'acclarata dimostrazione dell'inefficacia di pratiche alternative si faccia riferimento al capitolo "Problematiche di sicurezza nelle tecnologie adottate attualmente".
   Per l'impossibilità di abusi e circoscrizione dei dati si faccia riferimento alla descrizione tecnica che dispone della limitatezza dell'elaborazione da un punto di vista del dato (singola impronta), della

locazione (solo all'interno del device) e temporale (solo per pochi secondi).

4. Deroga motivata con uso controllato in speciali casistiche e non uso generalizzato o incontrollato o indifferenziato. Tale deroga motivata va periodicamente riesaminata, valutando la persistente sussistenza dei fattori che l'hanno determinata, anche alla luce del progresso scientifico.
   L'uso non è generalizzato, attiene solo al personale che opera in manutenzione sul database del Libro fondiario e limitatamente alla gestione di autenticazione e gestione dei diritti di accesso allo stesso.
5. Delimitata memorizzazione su circoscritti supporti correlati sempre disponibili per l'interessato e non centralizzazione sotto qualsiasi forma ed in particolare divieto assoluto di archivi centralizzati, anche se con dati cifrati. In particolare occorre attivare una funzione permanente di ricerca di soluzioni che evitino accumulazioni o unificazioni di dati.
   I dati biometrici sono circoscritti alla smart card e solo per pochi secondi replicati nel sistema di confronto biometrico e comunque non vengono accumulati o unificati essendo presenti unici nel device biometrico per un periodo temporale limitato a pochis econdi. I dati non vengono memorizzati in nessun archivio locale o centralizzato ma sono conservati solo nel supporto dato in uso esclusivo uso al proprietariod egli stessi. La smart card rimane sempre nella disposizione dell'interessato anche nel momento della lettura può essere asportata senza blocchi.
6. Temporanea conservazione in ordine cronologico per il necessario periodo limitato (e, come nel caso di associazione di dati biometrici con videoregistrazioni, per non oltre una settimana). Sono vietati, in particolare, le cosiddette copie di sicurezza che prolungano surrettiziamente i tempi di conservazione.
   I dati vengono conservati sul device per il tempo dell'autentica, massimo 6 econdi. In nessun caso vengono archiviati. Non esistono copie di sicurezza e organizzativamente vi è un regolamento che vieta l'emissione di smart card multiple per utente con obbligo di ritiro di quelle guaste.
7. Scrupolose misure di sicurezza con sistemi inequivoci e senza rischio, promuovendo, come obbligatoriamente ed inderogabilmente infatti nel caso di uso congiunto di dati biometrici e di videosorveglianza in banca, l'interposizione di un "vigilatore dei dati" indipendente, individuato nel titolare di una funzione in posizione di indipendenza o da un soggetto indipendente (anche proceduralmente non essendo designato dall'organo ammninistrativo bensì dall'organo indipendente). In particolare nei casi prescritti va evitata anche la sola teorica possibilità di decifrare le informazioni acquisite senza l'intervento di tale vigilatore.
   Come specificato nel capitolo di descrizione tecnica del sistema i dati sono mantenuti nella massima sicurezza. Le smart card contengono dati che usano una chiave composita che non è nella disponibilità del produttore del software e del gestore dell'impianto. Nessuno dei due soggetti può singolarmente prelevare i dati dalla smart card. Una delle due chiavi può essere definita dal "vigilatore dei dati" rendendo il suo consenso obbligatorio per qualsiasi operazione di verifica dei dati crittografati.
   L'algoritmo di crittografia è uno standard di mercato utilizzato dai maggiori enti pubblici mondiali.
8. Piena ed immediata conoscibilità dei dati biometrici da parte dell'interessato e limitazioni stringenti (sino al completo divieto nel caso di uso incrociato di dati biometrici e videosorveglianza) per datore di lavoro, suoi dipendenti e collaboratori. Per le operazioni inerenti alla conoscenza, va promossa, ove necessaria, la cooperazione di un vigilatore indipendente (obbligatorio e inderogabile nel caso di uso incrociato di dati biometrici e videosorveglianza).
   L'interessato dispone di tutti i dati biometrici gestiti essendo completamente contenuti nella smart card che è nella sua esclusiva disponibilità. L'uso degli stessi è ristretto alla funzione di autentica per l'assegnazione dei diritti di accesso al software di gestione del Libro fondiario della provincia di Bolzano. In nessun caso è previsto un uso diverso degli stessi in questo progetto.
9. Rispetto rigoroso degli obblighi di notifica al Garante (art. 37 Codice Privacy).
   Una volta completata la stesura del progetto definitivo verrà effettuata notifica al Garante sull'installazione di tale sistema.
10. Disattivazione automatica, immediata e certa di funzioni di smart card o altre analoghe nel caso di smarrimento o di furto.
    a. In caso di smarrimento o furto le credenziali dell'utente legate a quella smart card sono disabilitate rendendo la stessa inutilizzabile anche dall'utente stesso.
    b. Il regolamento prevede di consegnare la carta in caso di guasti e la sua distruzione

c. I dati presenti sulla carta sono crittografati e il suo contenuto non è estraibile da parte di un estraneo e nemmeno dal produttore o dal gestore.

(D) *Finalità (art. 2)*

Lo scopo del trattamento riguarda esclusivamente il controllo dell'accesso, mediante autenticazione, all'applicazione di gestione del Libro fondiario della provincia di Bolzano.

(E) *Principio di necessità nel trattamento dati (art. 3)*

Per la necessità si fa riferimentoa quanto riportato nel capitolo "Sensibilità del database e problematiche di sicurezza". Per la riduzione al minimo si fa riferimento a quanto detto nella descrizione tecnica in particolare a quanto previsto per la localizzazione dell'elaborazione e i stringenti limiti temporali nella conservazione dei dati.

(F) *Modalità di trattamento e requisiti dei dati (art. 11)*

In generale si fa riferimento a quanto detto nella descrizione tecnica.

a) Trattati in modo lecito e secondo correttezza; Per la liceità del trattamento e la correttezza si fa riferimento all'osservanza di quanto riportato nel codice della privacy in particolare il sistema costituisce una misura minima di sicurezza come specificato nell'art. 34, comma 1, lett. a del codice sulla privacy, e a quanto previsto dall'allegato tecnico che individua le caratteristiche biometriche come sistema previsto di autenticazione informatica.

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; prescrizione adottata integralmente come specificato sopra.

c) Esatti, se necessario, aggiornati; garanzia derivata dalle procedure organizzative e di gestione di guasti, furti eo smarrimenti.

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; i dati trattati sono quelli minimi necessari per l'operazione di autenticazione, il sistema biometrico memorizza e tratta solo il template, una credenziale e un codice di controllo.

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. I dati sono memorizzati solo nella smart card nell'esclusiva disponibilità dell'interessato che può in qualsiasi momento provvedere alla distruzione degli stessi e non solo alla fine del lperiodo d'uso.