

# Controllo accessi: *e se entrassi io al posto tuo?*

“L'uso di badge e transponder per identificare in modo automatico le persone nei sistemi elettronici di controllo accessi non è per nulla sicuro. Questi “oggetti”, infatti, si prestano potenzialmente a commettere diversi reati (anche gravi). Come entrare in un'area riservata o a rischio al posto di un collega, usufruire di un servizio che non spetta, attestare la falsa presenza al lavoro... Se la biometria (che garantirebbe la massima certezza d'identificazione) non è sempre consentita per via della privacy (oltre che dei costi), si può fare qualcosa per arginare il problema dello scambio del badge, malcostume sempre più diffuso?”

La tecnica più usata per identificare le persone nei sistemi elettronici di controllo accessi si basa sulla lettura di un “oggetto” che l'utente porta con sé e presenta, prima di entrare (o uscire), al lettore installato in corrispondenza di una struttura fisica che impedisce il libero transito. L'oggetto (*token*) può essere costituito da un badge nel classico formato carta di credito oppure, negli impianti basati su tecnologia RFid (Radio Frequency Identification), anche da un transponder a forma di portachiavi, ciondolo, orologio, braccialetto e simili. Questo metodo di riconoscimento è chiamato “indiretto” poiché il sistema non identifica la persona ma ciò che essa presenta, che dice di essere. L'unica soluzione in grado di garantire certezza d'identificazione, si sa, è la tecnologia biometrica (verifica delle impronte digitali, della topografia della mano ecc.) la quale, però, oltre a comportare un maggior costo, presenta numerose limitazioni d'impiego legate alla privacy.



Il reato più frequente legato al badge, sia negli enti pubblici che nelle imprese private, è quello di truffa per falsa attestazione della presenza al lavoro. Nelle grandi organizzazioni il fenomeno dei "furbetti del cartellino" si sviluppa e s'ingrossa grazie ai numerosi "contoterzisti", coloro che dietro compenso o meno sono disposti a timbrare per conto di colleghi (Courtesy Elex srl Torino)

## Il biochip RFID

Il principale problema del riconoscimento indiretto è dunque quello di non essere in grado di garantire certezza nella verifica dell'identità individuale. Nulla impedisce, infatti, che un utente, il quale deve accedere a un'area riservata o ad alto rischio, usi il badge di un'altra persona - con conseguenze facili da immaginare. In alcune realtà, come ad esempio le case di riposo per anziani affetti da particolari patologie, l'ostacolo può essere superato usando **un braccialetto da polso non rimovibile in cui è incorporato un chip RFID oppure una smart label impermeabile cucita** su un indumento del paziente. Ana-

logamente alcune tipologie di controllo accessi veicolare prevedono che il transponder sia costituito da un blocchetto waterproof fissato saldamente al telaio dell'automezzo o da un'etichetta autoadesiva da applicare al parabrezza e che, in caso di rimozione, l'effrazione balzi evidente all'occhio. Una soluzione tecnica per garantire certezza nell'identificazione delle persone senza ricorrere alla biometria ci sarebbe, ma aprirebbe questioni inquietanti sul fronte etico: basterebbe, infatti, impiantare un chip RFID sottopelle, tipicamente nel dorso della mano.

## Sette comandamenti da rispettare per chi detiene il badge



# Scambio di badge

**Scambio di badge:  
il prezzo da pagare per  
il dipendente (o l'azienda)**

- Ammonizione, sanzione, licenziamento o detenzione per truffa e altri reati ai danni dello Stato o dell'impresa privata (pena commisurata alla gravità)
- Rischio in termini di sicurezza fisica e logica a causa dell'appropriazione di diritti d'accesso altrui
- Danno economico per l'erogazione di servizi fruiti ma non spettanti
- Falsa ricostruzione dei movimenti in caso di incidenti a causa dell'errata associazione degli eventi (entrate, uscite, tentativi di accesso ecc.) a un utente
- Difficoltà in caso di evacuazione per emergenza a causa della falsa situazione del personale presente nel fabbricato (lista in real time)
- Possibili complicanze a livello assicurativo Inail in caso di infortuni fuori sede.

## I furbetti del badge

Lo scambio d'identità determinato dalla cessione fraudolenta del badge è un problema molto sentito nelle fabbriche e negli uffici, sia per le implicazioni di carattere giuridico, sia per gli aspetti connessi alla sicurezza fisica e logica. In questi ultimi decenni la legge è intervenuta più volte in materia comminando sanzioni anche molto pesanti. Il fenomeno più diffuso è quello noto come "i furbetti del cartellino", il dipendente che registra la presenza al lavoro di un collega mentre questi se ne sta beatamente a casa o altrove. I reati accertati e sanzionati sono ormai migliaia in tutta Italia. Oltre a costituire una truffa nei confronti dello Stato o dell'impresa privata, questa cattiva pratica ha **ripercussioni importanti anche nel versante safety e security**. La situazione dei presenti/assenti nell'ambito di un edificio, fornita in real time dal sistema e utile per la gestione delle emergenze, ad esempio, risulta falsata rispetto a quella effettiva. Così come non risulta corretta l'attribuzione dei DPI o di altri servizi nei casi in cui gli stessi vengono erogati in modo automatico.

## Si può fare qualcosa?

La domanda che spesso ci si pone è: si può fare qualcosa per contenere il fenomeno dello scambio dei badge negli ambienti di lavoro? Qualcosa si può e si deve. Molte imprese, ad esempio, al momento in cui si dotano di un sistema elettronico di controllo accessi, distribuiscono i badge (o i transponder) al proprio personale in modo del tutto informale. Il rilascio **del dispositivo di riconoscimento, personalizzato individualmente e accompagnato da una sottoscrizione di responsabilità** da parte del dipendente, è certamente una misura di prevenzione che funziona. Non si tratta altro che di una lettera da far firmare al momento della consegna del dispositivo e in cui il destinatario prende atto che il badge è un documento di riconoscimento personale di proprietà aziendale, che non deve essere alterato, ceduto a terzi o impiegato per usi impropri o illegali. Altre misure che si sono rivelate efficaci sono la verifica a sorpresa dell'effettiva presenza in azienda per quei soggetti avvezzi ad affidarsi ai colleghi per registrare gli accessi, l'uso di varchi che consentono il transito di una persona alla volta (tornelli, bussole ecc.) con integrata la funzione di anti pass back e l'installazione di un impianto di videoripresa nelle aree d'ingresso/uscita.



Il badge (o il transponder) in uso nel controllo elettronico degli accessi può prestarsi per impieghi impropri o illegali. A parte l'utilizzo della card per raschiare il ghiaccio dal parabrezza dell'auto (vivamente sconsigliato), basta il semplice scambio della stessa tra colleghi per incorrere in uno o più reati gravi: falsificazione d'identità, falsa attestazione di presenza, abuso nei diritti di accesso, fruizione di servizi non spettanti ecc.

## Cinque suggerimenti alle aziende

- 1**  
Personalizzare il badge (con logo, dati anagrafici, foto ecc.) dandole la parvenza di un vero e proprio documento d'identità personale
- 2**  
Accompagnare la consegna del badge con una lettera personalizzata, da far sottoscrivere al dipendente, contenente le istruzioni e le limitazioni d'uso
- 3**  
Utilizzare, ove è possibile, transponder non rimovibili come braccialetti da polso, etichette da cucire agli indumenti o da applicare al parabrezza dei veicoli
- 4**  
Fare verifiche a sorpresa (controllando le situazioni fornite in tempo reale dal sistema) del fatto che le persone avvezze a scambiarsi il badge sono effettivamente entrate e presenti
- 5**  
Impiegare barriere d'ingresso che consentano il transito di una persona alla volta (tornelli, varchi motorizzati ecc.) e installa sistemi di videoripresa nei punti più critici.