

Sistema di controllo accessi ad altissima sicurezza

www.efunds.com

La società E-Funds d.o.o. ha vinto all'inizio dell'anno un appalto di servizio per la gestione di carte di credito conformi allo standard EMV della VISA per Slovenia. Era richiesto che nel laboratorio dove si gestiscono queste tessere si installi un sistema di controllo accessi che garantisca l'identificazione certa di un soggetto e che nella zona presidiata si entri ed esca a coppie. Le richieste apparentemente semplici di VISA hanno comportato la realizzazione di un sistema complesso basato su lettori biometrici e RFID.

Le richieste apparentemente semplici di VISA hanno comportato la realizzazione di un sistema complesso basato su lettori biometrici e RFID.

L'ESIGENZA

La società slovena E-Funds d.o.o. ha vinto all'inizio dell'anno un appalto di servizio per la gestione di carte di credito conformi allo standard EMV (www.emvco.com) della VISA per la Slovenia. Il servizio di gestione delle carte di credito prevede l'inizializzazione delle smart card con l'installazione delle applicazioni EMV per l'interfacciamento coi circuiti interbancari per i pagamento e la modifica dei codici di sicurezza PIN e PUK. La VISA (www.visa.com) impone ai gestori regole di sicurezza molto rigide. Tra queste, si richiede che nel laboratorio dove si gestiscono queste tessere si installi un sistema di controllo accessi che garantisca l'identificazione certa di un soggetto (tramite verifica dell'impronta digitale) e che nella zona presidiata siano presenti sempre due persone, ovvero che l'accesso alla zona sicura si entri ed esca a coppie.

Per la realizzazione della zona sicura la E-Funds ha scelto la società Infodata Sistemi s.r.l., perché era già accreditata come fornitore di qualità per le carte di credito della DINERS e perché aveva già referenze di realizzazioni di sistemi di controllo accessi progettati su misura.

LA SOLUZIONE.

Le richieste apparentemente semplici di VISA hanno comportato la realizzazione di un sistema complesso basato su lettori biometrici e RFID.

La soluzione installata esige che per aprire la porta devono autenticarsi in contemporanea due persone su due lati diversi della porta, prima con il badge RFID e poi con l'impronta digitale.

Per accedere all'area sicura bisogna autenticarsi due volte per aprire le porte blindate. Per uscire devono autenticarsi sempre due persone autorizzate altrimenti restano nella zona sicura, nel caveau, con muri di cemento armato spesso oltre 1m. Ad ogni autenticazione vengono fotografati da una telecamera.

Dopo l'analisi delle caratteristiche richieste l'Infodata ha realizzato un progetto per il sistema di controllo accessi prevedendo quattro fasi: modifiche edili, installazione dell'impianto elettrico e del hardware, l'installazione di un software personalizzato e infine il collaudo del sistema.

Per la prima fase del progetto che riguardava le modifiche edili, si è deciso valutando le specifiche richieste e dopo un sopralluogo della zona da mettere in sicurezza di realizzare un doppio varco per accedere alla zona presidiata. L'idea del doppio varco è nata prendendo spunto da un altro sistema di controllo varchi: l'uscita da parcheggi con doppia sbarra, che garantiscono l'uscita singolare di ogni autovettura.

Nella seconda fase si è scelto i terminali per il controllo accessi valutandone le funzionalità e le caratteristiche richieste per l'installazione. La scelta è andata sui dispositivi iGuard (www.iguardsystem.it), e, precisamente sul modello LM520-FSC con lettore biometrico e RFID. Questi

utilizzato dei normali rel?ma dei rel?odificati, gli iG-ER-01, interfacciati all'iGuard tramite un BUS485. In questa modalit?e elettro-serratura non vengono eccitate dai rel?ei lettori iGuard, ma dai rel?sterni codificati, che sono installati in un box chiuso all'interno della zona presidiata: dopo l'autenticazione con gli iGuard viene inviato un segnale codificato via RS485 ai rel?odificati. Per garantire la conformit?el sistema ai requisiti richiesti, abbiamo installato anche dei sensori magnetici collegati agli iGuard: questi rilevano se una porta ? aperta o chiusa. In questo modo l'iGuard pu?viare un segnale d'allarme nel caso una porta risulti aperta. Infine, al sistema sono state aggiunte delle telecamere IP della AXIS (www.axis.com) con due finalit?ntrodurre anche una videosorveglianza classica e creare un database di foto di tutte le persone che entrano o escono dalla zona presidiata: in questo modo si pu?nitorare anche con certezza che non entrino persone non autorizzate nell'area sicura. Le IP camere scelte sono state le AX207; anche se sono le pi?conomiche? in casa AXIS, hanno caratteristiche sufficienti per la finalit?l progetto. La terza fase ha previsto la configurazione dei dispositivi iGuard e l'installazione di un software installato su un server. La gestione del sistema di controllo accessi avviene con un'interfaccia web del software installato direttamente negli iGuard, mentre il software server si occupa semplicemente di fare il backup dei dati degli accessi su un database locale e di salvare i video e le immagini fornite dalle camere AXIS. IL VANTAGGIO. Tramite un qualsiasi Internet browser ? possibile ottenere tutti i dettagli degli accessi, del tempo di permanenza nella zona sicura, dei tentativi d'accesso non autorizzati e di tutte le eventuali anomalie, e, di modificare le politiche d'accesso applicate agli operatori coinvolti. Con questo sistema la modalit?'accesso avviene attualmente con i requisiti richiesti: per aprire la prima porta due persone si devono autenticare tramite la verifica dell'impronta digitale in sequenza e in un tempo limitato (15 secondi); dopo l'apertura della porta entrano in un disimpegno tra due porte; per poter aprire la seconda porta, accedendo alla zona sicura, devono chiudere la prima porta e autenticarsi nuovamente entrambi sulla seconda porta. Per uscire le due persone devono effettuare la stessa procedura nell'altro verso, anche per garantire che non rimanga nella zona presidiata una sola persona. Il sistema installato ? stato collaudato e certificato dalla VISA come conforme ai requisiti sulla sicurezza di impianti per la gestione di carte di credito EMV, diventando cos?nche un modello utilizzabile da tutti i service bureau impegnati nella stessa attivit?l case study ? pubblicato sul numero di giugno della rivista Essecome.