appunti

Un computer in tasca

Le smart card sono dotate di microcontrollore, sistema operativo, effettuano operazioni logiche, calcoli matematici...

MATTEO MARINO

Le smart card sono corredate da uno o più circuiti integrati e sono in grado di sfruttare diverse tecnologie per l'acquisizione delle informazioni. I dati possono essere prelevati attraverso tecnologie basate su bande magnetiche, codici a barre (lineari o bidimensionali), sistemi a radiofrequenza con lettura a distanza, parametri biometrici e di autenticazione. I circuiti integrati (ICC, Integrated Circuit Chip) nelle smart card agiscono come micro-controllori o computer e le informazioni nelle memorie del chip sono utilizzabili per numerose applicazioni. La memoria ospita, inoltre, chip dedicati al governo del sistema operativo (COS, Chip Operative System), software adibiti alle comunicazioni e algoritmi per la codifica e decodifica dei dati crittografati.

Alcune applicazioni

Il controllo degli accessi costituisce probabilmente una delle applicazioni più diffuse e conosciute della tecnologia smart card. Le smart card possono, infatti, essere utilizzate come mezzo attraverso il quale identificare e controllare rapidamente il personale per la verifica sia dell'accesso fisico negli uffici, edifici o locali sia dell'accesso verso reti locali, sistemi condivisi, ecc. In funzione della specifica capacità del chip integrato, le smart card possono arrivare a storicizzare grandi quantità di informazioni. Una delle ultime frontiere della tecnica di soccorso prevede, per esempio, l'utilizzo delle smart card per memorizzare i dati dei pazienti. Tale 'cartella clinica portatile' è in grado di fornire, mediante adeguati lettori, un quadro clinico completo in pochi secondi ai medici che ne richiedessero i contenuti.

Le smart card sono corredate da uno o più circuiti integrati e sono in grado di sfruttare diverse tecnologie per l'acquisizione delle informazioni

In tutti i casi di pronto intervento, attraverso smart card in possesso degli assistiti, è possibile fornire ai medici in pochi attimi un'esaustiva condizione dei pazienti riducendo significativamente i rischi determinati da soccorsi tardivi. La tecnologia smart card è in grado di migliorare i processi di gestione della sicurezza aziendale attraverso l'identificazione del personale e dei clienti sfruttando sistemi di acquisizione rapida. La memorizzazione in tempo reale e il governo delle informazioni a essi pertinenti favorisce, inoltre, tutte le fasi di tracciatura, di supporto e di comunicazione. Gli evoluti sistemi biometrici di identificazione e le infrastrutture PKI (Public Key Infrastructure) possono elevare significativamente la sicurezza grazie anche alle chiavi pubbliche e private con cui generare codici crittografici per occultare e proteggere le informazioni sensibili come la firma digitale o i contenuti delle mail. La tecnologia asseconda, inoltre, i bisogni espressi dal settore della 'identificazione' soddisfacendone efficacemente i requisiti attraverso gli strumenti di controllo degli accessi (ACT, Access Control Tool), di pagamento, di storicizzazione delle informazioni, ecc.

I dispositivi di lettura e scrittura delle smart card determinano il collegamento fisico tra le card e i sistemi di gestione delle informazioni. Tali apparecchiature possono essere costituite da PC, da sistemi di rete o da dispositivi standalone come i sistemi di controllo degli accessi

Chip Card

Nonostante sia di uso comune parlare delle smart card utilizzando impropriamente i termini chip card, circuiti integrati e smart card, le chip card sono classificabili sia attraverso il tipo di chip che le equipaggia sia mediante l'interfaccia di trasmissione utilizzata per la comunicazione con il lettore delle informazioni. I tre tipi di chip che possono essere installati sulle card sono di sola memoria, di tipo wired logic e i microcontrollori. Le card con circuito integrato di sola memoria, che includono anche quelle con sistema di protezione seriale, sono contraddistinte dalla memorizzazione a banda magnetica. I due vantaggi principali di questo tipo di chip card sono l'elevata capacità di memoria e l'economicità dei sistemi di lettura e scrittura che si utilizzano per l'acquisizione delle informazioni memorizzate. Tali chip card sono solo in grado di memorizzare informazioni senza poter effettuare nessun tipo di operazione logica o di calcolo mentre le card con protezione seriale si distinguono dalle prime solo per un più elevato livello di sicurezza. Mentre le prime versioni delle chip card di sola memoria non erano in grado di assicurare un elevato livello di sicurezza, le attuali card di questo tipo sono corredate da evoluti schemi di autenticazione logica per salvaguardare le informazioni oltre che da sistemi di identificazione numerica personale (PIN, Personal Identification Number) con i quali proteggere i dati di credito eventualmente storicizzati sui dispositivi. Le chip card a circuito integrato di tipo wired logic sono in grado di discriminare gli accessi alle informazioni memorizzate attraverso protezioni di autenticazione crittografata. Le card di questo tipo sono, inoltre, capaci di fornire un file system di tipo statico che supporta numerose applicazioni. Il file system e il corredo di comandi delle wired logic card sono modificabili attraverso la riprogrammazione del circuito integrato. Il terzo tipo di chip card è costituito dai microcontrollori che rappresentano il sistema più dotato, sicuro e completo rispetto ai precedenti. Le card di questo tipo sono equipaggiate con un microcontrollore, con un sistema operativo e con una memoria di tipo lettura/scrittura aggiornabile per numerosi cicli. Le card con microcontrollore possono effettuare operazioni logiche e calcoli matematici memorizzando una grande quantità di dati in accordo con le funzionalità dal sistema operativo. Tali sistemi, grazie alle specifiche potenzialità di calcolo, possono essere paragonati a PC in miniatura che richiedono solo l'alimentazione e terminali idonei alla comunicazione. Nonostante si utilizzi genericamente il termine di smart card per tutti i sistemi di memorizzazione delle informazioni su chip card, le smart card sono costituite solo da quest'ultima tipologia di dispositivo dotata di microcontrollore. In commercio sono attualmente disponibili chip card di ultima generazione con e senza contatto oltre che sistemi con circuito integrato a doppia interfaccia. Diversamente dai prodotti di sola memorizzazione, tali circuiti integrati con microcontrollore possono essere

Gli evoluti sistemi biometrici di identificazione elevano la sicurezza attraverso le chiavi pubbliche e private con codici crittografici in grado di occultare e proteggere le informazioni

impiegati per scopi specifici ove il livello di sicurezza da rispettare sia particolarmente elevato.

I dispositivi di lettura e scrittura

I dispositivi di lettura e scrittura delle smart card determinano il collegamento fisico tra le card stesse e i sistemi di gestione delle informazioni. Tali apparecchiature possono essere costituite da PC, da sistemi di rete o da dispositivi standalone come i sistemi di controllo degli accessi.
Tali apparati provvedono all'inizializzazione delle card oltre che alla fornitura dell'alimentazione necessaria al loro funzionamento. In funzione del tipo di interfaccia con cui le card sono equipaggiate, il trasferimento della corrente è effettuato attraverso il contatto fisico o la trasmissione radio mediante le antenne predisposte sui dispositivi. L'inizializzazione delle smart card è costituita da un processo istituito dagli appositi lettori per cui è sempre necessario verificare preventivamente se tali apparecchiature siano in grado di effettuare un'idonea predisposizione. I sistemi di lettura e scrittura, cui le smart card si collegano, possono essere costituiti, oltre che da semplici dispositivi di collegamento tra i PC e le tessere (trasparent device), da apparecchiature con caratteristiche elaborative totalmente indipendenti capaci di acquisire, memorizzare e gestire tutti i dati prelevati dalle card intraprendendo, inoltre, il trasferimento delle informazioni verso le smart card stesse. Dal punto di vista trasmissivo tali apparati possono essere paragonati ai PC soft modem per i quali il contenuto software costituisce una componente determinante per il buon esito delle comunicazioni da e verso le smart card. Effettuando un confronto tra i sistemi di lettura/scrittura descritti si evidenzia che mentre gli apparati indipendenti sono in grado di gestire autonomamente il flusso delle informazioni provenienti dai sistemi a cui sono connessi per un trasferimento efficace verso le smart card, i dispositivi 'trasparenti' non possiedono capacità elaborative. Tale limite è però compensato dalla convenienza economica offerta, favorevole sia durante le installazioni massive sia nelle fasi di manutenzione. Nella scelta del tipo di installazione da effettuare è importante considerare però che, sebbene gli apparati autonomi siano molto dispendiosi, possiedono sempre configurazioni dei driver idonee alla gestione automatica della comunicazione con i lettori. Tale aspetto acquisisce un'importanza rilevante soprattutto durante le fasi di aggiornamento dei software per migliorare le prestazioni dei sistemi. Nonostante in commercio sia possibile acquistare smart card e sistemi di lettura e scrittura relativamente economici, è importante, durante le fasi di progettazione di interi apparati, effettuare considerazioni non solo legate al costo dell'acquisto ma anche all'economia a vita intera degli impianti. I sistemi sviluppati e installati dovrebbero poter essere sempre conformi agli specifici requisiti e bisogni. In tali impianti è importante, inoltre, non trascurare il livello di affidabilità degli apparati hardware a causa delle sollecitazioni cui le smart card e dispositivi di lettura e scrittura solitamente sono soggetti. I lettori di smart card possono essere integrati con numerosi dispositivi anche attraverso tecnologie di interfacciamento consolidate come USB,

Caratteristiche

Standard	ISO/IEC 14443 ISO/IEC 15693	ISO/IEC 7810 ISO/IEC 7810	 125 kHz
Frequenze	13.56 MHz	13.56 MHz	125 kHz
Intervallo di lettura	Fino a 100 mm	Fino a 1 m	Fino a 1 m
Tipo di chip supportato	Memory Wired logic Secure microcontroller	Memory Wired logic	Memory Wired logic
Funzioni di autenticazione	MIFARE encryption, DES/3DES, AES, RSA, ECC	Supplier-specific, DES/3DES	Supplier-specific
Intervallo di memoria	64 to 72 Kb	256 and 2 Kb	8 to 256 b
Capacità di lettura/scrittura	lettura/scrittura	lettura/scrittura	solo lettura
Velocità di trasmissione (Kb/s)	Fino a 106 (ISO) Fino a 848 (available)	Fino a 26.6	Fino a 4
Anti-collision	Si	Si	Opzionale
Autenticazione Card-to-reader	Challenge/Response	Challenge/Response	Password
Card ibride	Si	Si	Si
Supporto Contact interface	Si	No	No
Compatibilità GSC-IS	Si	No	No

porte seriali, Pcmcia, ecc. oltre ad adattarsi a installazioni di ogni tipologia. Ne sono un esempio le integrazioni con i dispositivi PDA o le installazioni dei sistemi di controllo degli accessi per i quali gli intercettori sono solitamente collocati sugli accessi affinché le interfacce senza contatto acquisiscano le informazioni dei passaggi in modo trasparente agli utenti. I dispositivi di scrittura delle smart card sono solitamente utilizzati per effettuare la personalizzazione delle tessere. Tali apparecchiature sono in grado, infatti, di inizializzare le smart card effettuando contemporaneamente la personalizzazione dei chip; tale caratteristica assicura il completo rispetto della coerenza delle informazioni delle card.

Interfacce

I sistemi con e senza contatto costituiscono le due principali interfacce delle chip card. I due differenti sistemi sono responsabili sia dell'alimentazione a favore del circuito integrato (Integrated Circuit Chip) sia del trasferimento delle informazioni dal circuito stesso verso i dispositivi di lettura. In commercio sono, attualmente, disponibili carte con la duplice funzionalità che sfruttano un impianto con doppio chip (hybrid card) o con doppia interfaccia (combo card). Mentre le smart card di tipo a 'contatto' richiedono l'inserimento delle tessere in appositi sistemi di lettura dotati di connessione diretta per il trasferimento delle informazioni, le smart card di tipo 'contactless' sono in grado di effettuare la migrazione o l'acquisizione dei dati mediante il semplice avvicinamento dei supporti ai dispositivi di lettura. Le antenne installate sia sui sistemi di lettura sia sulle card stesse rendono possibile il trasferimento delle informazioni attraverso onde in radio frequenza (RF, Radio Frequency) o per induzione entro distanze dipendenti dalla tipologia di sistemi trasmissivi e dagli standard utilizzati. Le smart card di tipo ibrido sono equipaggiate con due chip solitamente non fisicamente interconnessi che supportano rispettivamente le interfacce con e senza contatto mentre le più evolute card 'dual interface' sono in grado di ricevere e inviare le informazioni attraverso entrambi i tipi di lettore. Grazie alle elevate prestazioni dei chip con interfaccia senza contatto, essi sono utilizzati efficacemente in tutte le applicazioni ove è richiesta l'acquisizione e la lettura veloce delle informazioni come nel controllo dei passaggi con portata elevata, degli accessi agli edifici, ecc. I sistemi senza contatto sono caratterizzati da un'elevata durata rispetto agli omologhi dispositivi a strisciamento grazie all'usura limitata cui sono soggetti. Indipendentemente dall' interfacciamento adottato da tali sistemi, la comunicazione istituita con chip facilmente trasportabili è utile e applicabile in svariate situazioni. Ne sono un esempio le tre principali tecnologie utilizzate per il controllo degli accessi identificate come la ISO/IEC 14443, la ISO/IEC 15693 e la 125 kHz. Le smart card con tecnologia a 13,56 MHz sono basate sugli standard ISO/IEC 14443 e ISO/IEC 15693. Tale tipo di smart card è compatibile con i più evoluti strumenti di lettura e scrittura autenticando l'identità delle persone in possesso delle tessere, determinando il livello di accessibilità alle strutture e conferendo l'idoneità all'accesso specifico in funzione dei permessi conferiti. Tali card possono contenere ulteriori fattori di autenticazione come codici PIN o parametri biometrici oppure chip aggiuntivi a contatto per soddisfare esigenze specifiche di integrazione con tecnologie legacy. La norma ISO/IEC14443 è stata sviluppata compatibilmente con lo standard dei chip a contatto ISO/IEC 7816 perché determini un trasferimento idoneo a distanze al di sotto dei 100 mm tra il lettore e il chip. Per tale tipo di standard, risulta, infatti, impossibile trasferire l'energia necessaria al funzionamento del chip anche attraverso un'antenna di elevata portata. Lo standard ISO/IEC15693 fu creato specificatamente per soddisfare i requisiti del settore della logistica, dell'ambito dell'etichettatura oltre che per abbracciare le necessità tipiche del settore agricolo per il quale è necessario trasferire poche informazioni a grandi distanze. ISO/IEC15693 non è compatibile con la norma ISO/IEC7816 per cui i prodotti conformi a tale standard non permettono l'acquisizione dei dati attraverso strumentazione di tipo a contatto. La tecnologia 125 KHz è compatibile con strumenti a radio frequenza di sola lettura utilizzati oggi per impieghi di controllo degli accessi non normati da uno specifico standard internazionale ma sorretti maggiormente da una consuetudine industriale de facto. ■