

## KIM ACQUIRING

### La soluzione per il Key Management

Nell'ambito del progetto di migrazione delle carte di pagamento alla tecnologia a microchip, particolare rilevanza assume la gestione delle nuove quantità di sicurezza (chiavi, certificati, ecc.) necessarie per l'emissione e per l'autorizzazione.

Le quantità di sicurezza, definite dallo standard EMV, dall'Associazione Progetto Microcircuito e dalle Certification Authority dei circuiti di pagamento, riguardano l'autenticazione e l'autorizzazione delle carte da parte dei terminali e dei Centri Autorizzativi, la protezione dei dati scambiati tra terminali e centri autorizzativi, le attività di mutua autenticazione e invio da remoto di Master Key iniziale verso i terminali (Remote Key Loading).

#### SOLUZIONE

L'applicazione KIM (Key Management) di TAS rappresenta lo strumento ideale per **consentire alle banche e ai centri servizi di gestire tutti gli aspetti legati alla generazione e alla gestione delle quantità di sicurezza e allo scambio di dati riservati tra le varie entità che operano nell'ambito del Progetto Microcircuito.**

KIM può essere utilizzato come repository generalizzato per tutte le chiavi che verranno gestite in base ai principi di dual control e split knowledge, tracciando le attività che gli utenti eseguiranno sulle chiavi stesse.

#### BENEFICI

La soluzione proposta da TAS, di facile implementazione e provata affidabilità, traduce in pratica la sempre maggiore attenzione rivolta al tema cruciale della sicurezza e **garantisce la piena conformità ai parametri di sicurezza** richiesti nell'ambito delle procedure di emissione e di autorizzazione delle carte e nello scambio di dati riservati.

#### FUNZIONALITÀ

- **Architettura a tre livelli** - Presentation, server dipartimentale (application) e server host
- **Interfaccia utente** - Interfaccia grafica web, user friendly, che guida gli utenti nella gestione di tutti i processi
- **Sicurezza** - Struttura modulare per i processi di autenticazione e autorizzazione, cifratura dei dati memorizzati, controlli applicativi su specifiche EMV e Progetto Microcircuito
- **Gestione dispositivi periferici** - Scambio dati nelle modalità richieste dalle entità coinvolte, mediante floppy disk o file system
- **Colloquio con apparato crittografico** - Utilizzo di un unico canale di colloquio con il crypto device (scheda IBM per OS390 o HSM di Thales e-Security) per veicolare le attività crittografiche legate a processi di generazione e gestione delle chiavi, a processi

autorizzativi e a processi di emissione delle carte

- **Registrazione eventi** - Tutte le funzioni svolte dagli utenti e gli eventuali errori sono registrati su apposito log, visualizzabile con differenti livelli di dettaglio
- **Multi-lingua** - L'interfaccia utente permette di scegliere l'italiano, l'inglese o altre lingue
- **Configurazione** - Applicazione dedicata per le funzioni di configurazione del prodotto

