

RKL

La soluzione che consente il Remote Key Loading per ATM

Il crescente utilizzo degli sportelli Bancomat da parte della clientela ha spinto le banche ad investire sempre di più sui prodotti che possano aumentare l'operatività degli ATM e, allo stesso tempo, diminuirne i costi di gestione. Inoltre, la necessità di incrementare gli standard di sicurezza, ha portato all'introduzione di algoritmi di cifratura a chiavi asimmetriche e relativi certificati rilasciati dalle Certification Authority abilitate nei circuiti di pagamento italiani ed internazionali.

SOLUZIONE

TAS, integrando i prodotti GEBA, KIM e il modulo Servente Sicurezza Operativa, ha sviluppato una soluzione di Remote Key Loading (RKL) che consente di **inviare in remoto tutte le chiavi operative ad uno sportello bancomat**, previa autenticazione di quantità cifrate con algoritmo RSA.

Allo scopo di accrescere ulteriormente la sicurezza, la soluzione permette di generare chiavi operative diverse per ogni ATM gestito e di non memorizzare tali chiavi in alcun archivio, rendendone di fatto impossibile un uso fraudolento.

BENEFICI

La soluzione proposta da TAS **aumenta la sicurezza elevandola ai più alti standard conosciuti** e nel contempo permette di **diminuire i costi di gestione degli ATM** evitando l'utilizzo di personale per le attività di installazione di uno sportello Bancomat.

La modularità e l'interoperabilità dei prodotti consente inoltre di proporre sul mercato la componente RKL che risiede sul Gestore Terminali ATM separatamente dalla componente di generazione delle chiavi asimmetriche (KIM) e dalla componente di generazione/verifica delle quantità di sicurezza (Servente Sicurezza Operativa).

FUNZIONALITÀ

- **Architettura a tre livelli** - Presentation, server dipartimentale e server host
- **Interfaccia utente** - Interfaccia grafica web user friendly che guida gli utenti nella gestione di tutti i processi
- **Gestione flusso applicativo** - Il prodotto può gestire tutti gli sportelli del gruppo bancario, implementando le specifiche di Remote Key Loading per il colloquio con i terminali
- **Sicurezza** - Struttura modulare per i processi di autenticazione e autorizzazione, cifratura dei dati memorizzati (Tripla DES e RSA), gestione dei certificati ISO9796-2, verifiche e firme digitali

- **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 ai processi di generazione/gestione delle chiavi e ai processi autorizzativi

