

## RKL

### The solution for ATM Remote Key Loading

The growing use of cash dispensers by customers is pressing banks to increase investments in solutions that empower ATM operations and curtail their management costs. Furthermore, the need to increment security standards has pushed the introduction of ciphering algorithms with asymmetrical keys and certificates released by the Certification Authorities of the Italian and International payment circuits.

#### SOLUTION

TAS has integrated the ATM Manager and Operating Security Server module and developed a Remote Key Loading (RKL) solution that **allows to remotely send all operational keys to cash dispensers**, subject to prior authentication of RSA algorithm ciphered quantities.

To further increase security, the solution allows to generate different operational keys for each ATM managed, without storing such keys and thus making fraudulent use virtually impossible.

#### BENEFITS

The solution proposed by TAS **increases security up to the highest known standards** to date and, at the same time, it allows to **cut-back ATM management costs**, not requiring the use of personnel for cash dispensers installation activities.

The modularity and interoperability of the products also allows to propose to the market the RKL component, which resides on the ATM Terminal Manager separately from the asymmetric key generation (KIM) and from the generation or check of the security quantities (Operating Security Server) components.

#### FEATURES

- **Tree-tier architecture** – Presentation, departmental server and hosting server
- **User interface** – User friendly graphic user interface, helping users in executing all the operations
- **Application flow management** – The product can manage all the bank machines, implementing the Remote Key Loading specifications for communicating with the terminals
- **Security** – Modular structure for the authentication and authorisation processes, ciphering of stored data (Triple DES and RSA), management of the ISO9796-2 certificates, checks and digital signature

- **Peripheral devices management** – Data Exchange in the ways requested by the involved entities, through floppy disk or file system
- **Communication with crypto device** – Use of a single communication channel with Crypto Device (OS390 IBM card or Thales e-Security HSM) to send the crypto activities linked to the key generation, management and authorizing processes.

# CHANNEL MANAGEMENT

