

KIM ISSUING

The Key Management solution

Within the migration project of payment cards to the microchip technology, particularly important is the management of the new security elements (keys, certificates, etc.) that are necessary for issuing and authorising operations.

Security elements, as defined by EMV standards, Microchip Project Association and payment circuits Certification Authorities, concern cards authentication and authorisation by terminals and Authorisation Centres, the protection of the exchanged data, the mutual identification activities, and the remote send of initial “Master Keys” to terminals (Remote Key Loading).

SOLUTION

KIM (Key Management) represents the ideal application for **banks and service centres to manage all the aspects related to the generation and management of security elements, and to the exchange of confidential data between the various operators of the Microchip project**. KIM may be used as general “repository” for all the keys, which will be managed in accordance with the “dual control” and “split knowledge” principles, tracking down the activities executed by users on their own keys.

BENEFITS

The solution, of easy implementation and proven reliability, puts into practice the constantly increasing attention paid to security aspects and **guarantees full compliance with the security parameters** requested when issuing and authorising cards, as well as in the exchange of confidential data.

FEATURES

- **Three-tier architecture** – presentation, application server and host server
- **User interface** – user friendly web graphic interface, guiding users in managing all processes
- **Security** – modular structure for authentication and authorisation processes, ciphering of stored data, application controls on EMV and Microchip Project specifications
- **Management of peripheral devices** – data exchange with the methods required by the involved actors, through floppy disk or file system
- **Dialogue with cryptographic system** – use of a single dialogue channel with the Crypto Device (IBM card for OS390

or HSM by Thales e-Security) to transmit the ciphering of keys generation and management to authorising and card issuing processes

- **Event recording** – all the operations executed by users as well as all errors, if any, are recorded on an appropriate log, that may be displayed with various levels of detail
- **Multi-language** – the user interface allows to choose among Italian, English or other languages
- **Configuration** – dedicated application for product configuration functions

CARD MANAGEMENT

