



# SAM



## A Secure Access

**Module** is the essential device for a secure and interoperable teleticketing system.

The security of a contactless system is based on secret keys used to authenticate transactions between the terminals and the cards. These keys are stored into the cards or tickets and into a Secure Access Module. A SAM is a smartcard installed permanently in the equipment interacting with the cards or tickets.

ASK is a pioneer of SAM management in Calypso and Mifare environments. Secure Access Modules contain cryptographic keys that are being generated during ASK's keys ceremonies and personalized for your specific application.

## SAM Secure Access Module

### Personalization of a full range of SAM

- CSAM-F
- SAM S1D4, S1D6, S1D7
- SAM S1E1, S20
- NXP Mifare SAM AV2

### Management of cards and tickets

- Calypso Rev1 / Rev2/ Rev 3 cards:
  - TanGO, CD21 (in all emulations)
  - CTS, CTM, SRT
- Mifare Classic™, DESFire, DESFire EV1, Mifare™ UL C, Mifare Plus™

### Key ceremony

- Ceremonies for Calypso systems
- Ceremonies for Mifare systems
- Security architecture definition
- Interoperability management
- Secure storage of master secret keys



calypso



## CSAM-F features

### Main features

- DES, DESX and TDES cryptographies
- Supports Calypso Rev1 / Rev2 and Rev3 cards
- Cryptographic keys management
- Data ciphering and unciphering
- Key usage counters and ceilings
- CTM anti-cloning algorithm

### Standards

- ISO 9797-1 MAC
- Designed to resist EAL4+ attacks

### Communication protocols

- ISO/IEC T=0 protocol
- High Speed Protocol (HSP)

### Other functions

- 26 event counters + PME
- Up to 255 work keys
- Lock/unlock keys diversification
- Variable signature size (2, 4, 6, 8 bytes)

### Characteristics

- ISO format with removable MicroSIM (ID000)
- Voltage supply: 2.7 to 5.5V
- Working temperature: -25°C to 60°C
- Storage temperature: -65°C to 60°C

## NXP Mifare SAM AV2 features

### Main features

- Secure download and storage of keys
- Supports MIFARE Ultralight, MIFARE Ultralight C, MIFARE 1K, MIFARE 4K, MIFARE Plus, MIFARE DESFire, MIFARE DESFire EV1
- Simultaneous multiple card support (up to 4 parallel sessions)
- MIFARE Crypto1
- TDEA (Triple DES encryption algorithm), AES-128, AES-192 cryptography
- RSA cryptography

### Standards

- SHA-1, SHA-224, SHA-226

### Communication protocols

- ISO 7816 T=1 protocol
- Support high speed baud rates up to 1,5Mbit/s

### Other functions

- MACing / Encipherment / SAM communication / Offline cryptography
- Signature generation and verification, RSA decryption for symmetric key updates
- 128 symmetric key entries, 3 RSA key entries
- 16 key usage counters and ceilings

### Characteristics

- ISO format with removable MicroSIM (ID000)
- Voltage supply: 3V or 5V
- Working temperature: -25°C to 60°C
- Storage temperature: -65°C to 60°C

