

VSAM

VSAM – Virtualization secure access module



Description

The SAM (Secure Access Module) is a plug-in format smart card that enhances the security and cryptographic performance in payment terminals, such as validators, for EMV contactless cards.

The VSAM (Virtualization SAM), like its sibling for closed-loop applications, the CL_SAM, extends these features by providing both open-loop and closed-loop payments. It embeds secure transaction processing, which enhances system security.

The VSAM also carries the EMV kernel L2, optimized for Visa “Online Deferred” transactions, and provides an interface with an EMV Level 1 certified contactless reader to perform all EMV transactions quickly and securely with easy implementation.

This means it can add EMV contactless card technology on top of legacy systems without

changing the validator application software or the automatic fare collection system back office.

The VSAM is remotely updatable, not only its internal tables but also in its software, using a secure method for both.

In addition to the EMV Kernel L2, the VSAM has the flexibility to support other EMV scheme kernels, making it a very powerful, secure, and customizable product.

Warranty

6 months

Partnumbers

- VSAM (I0285)

Applications

- Secure on-line and off-line payment system
- Public transportation EMV integration

Capabilities

The VSAM EMV Kernel L2 can handle:

- FDDA validation
- Expiration date
- EMV L2 validations
- VCPS (Visa Contactless Payment System) specification version 2.1.3
- Visa Ready MTT mobility and mass transit transaction specification, pre-authorized and deny lists.
- Can perform DDA validation for other brands.
- Provides an interface with the EMV Level 1 certified contactless reader based on APDUsv(Application Protocol Data Unit: the communication unit between a reader and a card) supporting all commands required for EMV contactless payment application.
- Uses the Mirror, Virtualization and Interception concepts.
- APIs to handle virtualization of MIFARE Classic over CIPURSE, MIFARE Plus and DESFire (secure card technologies).

Specifications

- **Power supply:**
ISO7816 standard
- **Dimensions:**
ID-1 (85.6 x 54 mm) with ID-000 plugin (25 x 15 mm)
- **Interfaces:**
ISO7816
- **Operating temperature:**
0 to 70°C
- **Further characteristics:**
 - CC EAL5+ certified hardware.
 - Ultra-fast hardware crypto engine.
 - Secure way to download keys into SAM based on its public key.
 - Each SAM may be registered by a Certificate Authority with a copy of its public key and CSN. The CA may be a trusted entity to support a multi issuer application.