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 – Patent pending), 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 na interface with na 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.

Remote Lifecycle Management: the VSAM supports secure remote updates, allowing for seamless upgrades of internal tables, software firmware, and key rotation. All updates are performed through a highly secure, encrypted methodology to ensure system integrity without physical intervention.

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.

The VSAM is the core of Planeta's EMV ecosystem, working in seamless integration with the SCR916 reader and the AIPA architecture. By hosting flag kernels directly within its secure environment, the VSAM ensures easy replication and high portability across diverse hardware setups. Engineered for maximum efficiency, it leverages the SCR916's high-speed interface to deliver peak processing performance for both EMV and closed-loop cards. Its non-intrusive AIPA-based design allows for agile operation in open or closed-loop systems, all while supporting full remote management for the loading of kernels, configurations, and updated lists.

Applications

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

Key advantages

- **Integrated EMV Ecosystem:** A unified, non-intrusive solution combining the SCR916, VSAM, and AIPA architecture for seamless open and closed-loop operations.
- **Certified Portability:** Preserves existing certifications across different platforms, drastically simplifying new integrations by requiring only a regression test.
- **Zero-Touch Management:** Future-proofs your business with full remote loading of kernels, configurations, and blacklists, eliminating the need for field intervention.
- **Advanced Closed-Loop & Hybrid Security:** Internally hosts both EMV and closed-loop applications, providing superior security and effortless migration between different media or platforms.
- **High Kernel Capacity:** Offers the flexibility to host approximately 8 independent kernels simultaneously, allowing for a diverse and evolving payment landscape.
- **Optimized Performance Interface:** Specifically engineered to leverage high-performance ISO7816 interfaces, such as those found on the SCR916, ensuring maximum transaction throughput.
- **Multi-Issuer Ready**: The SAM is perfect for ecosystems where different service providers (e.g., transport and payment) need to share the same secure environment.
- **Future-Proof:** The RSA 4096 and ECC 521 support ensures the product meets security standards for the next decade.
- **EAL5+ Assurance:** the hardware is government-grade secure.

Capabilities

The **VSAM EMV Kernel L2** can handle:

- VCTKS 1.1 (Visa Contactless Transit Kernel Specification)
- VCPS (Visa Contactless Payment System) specification version 2.1.3
- MasterCard 3.4
- American Express 4.1
- Discover (DPAS) 2.0
- JCB 1.6
- Interac
- FDDA validation
- Expiration date
- EMV L2 validations
- 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 APDUs (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).

Custom applications

Support for loading custom applications to the secure environment based on M^{2}ESA technology (patent pending).

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:
  - -25 to 85°C

Further characteristics:

- Security & Trust Architecture
  - Hardware Certification: Built on Common Criteria (CC) EAL5+ certified hardware for maximum tamper resistance.
  - Secure Provisioning: Features a highly secure method for downloading keys into the SAM based on its unique Public Key.
  - Identity & Traceability: Each SAM can be registered by a Certificate Authority (CA) with its Public Key and Chip Serial Number (CSN).
  - Multi-Issuer Support: Designed as a trusted entity to facilitate multi-issuer applications, allowing diverse providers to operate on the same infrastructure securely.
- Performance & Efficiency
  - Ultra-Fast Hardware Crypto Engine: Dedicated hardware acceleration for all cryptographic operations.
  - Processing Power: 50 MHz clock speed / 1 MByte Flash / 32 KBytes RAM.
  - Unmatched Speed: AES encryption in under 10µS.
  - Data transfer rates up to 1.25 Mbit/s.
  - Versatile Power: Dual-voltage operation (3V or 5V).
- Connectivity & form factors
  - Communication: ISO7816-3 (T=0 or T=1).
  - Physical Formats: Available in ISO7810, 2FF, and 3FF formats.
  - Application Ready: Full support for RISC-V client applications.
- Advanced Cryptographic Suite (Hardware-Based)
  - Symmetric Cryptography
  - Supports ECB, CBC, CTR, and GCM modes:
  - AES: 128, 192, and 256 bits.
  - DES / 3DES: 2K3DES, 2K3DES16, and 3K3DES.
  - DUKPT: Native support for DUKPT-3DES and DUKPT-AES (128/192/256).
  - Storage: Up to 128 symmetric and 3 RSA keys per directory.
  - Asymmetric Cryptography
  - RSA: 1024 up to 4096 bits (Encryption, Decryption, Signature, and On-chip Key Generation).
  - ECC (Elliptic Curve): 112 up to 521 bits (Supports 26 curves; Signature, Verification, and On-chip Key Generation).
  - Key Agreement: ECDH (secp256 and configurable curves) and Diffie-Hellman.
  - Storage: Up to 3 RSA key pairs per directory.
  - Hash & Integrity Functions
  - SHA: Full range support from SHA-1 to SHA-512.
  - Integrity: CRC 16/32 bit and CMAC diversification.
  - Certified Libraries: Pre-loaded with certified crypto libraries.

Part number

VSAM (I0285)

Warranty

12 months