VSAM

VSAM – Módulo de acceso seguro por virtualización

Descripción

El SAM (Módulo de Acceso Seguro) es una tarjeta inteligente enchufable que mejora la seguridad y el rendimiento criptográfico en terminales de pago, como validadores, para tarjetas EMV sin contacto.

El VSAM (SAM de Virtualización - patente pendiente), al igual que su equivalente para aplicaciones de bucle cerrado, el CL_SAM, amplía estas funciones al proporcionar pagos tanto de bucle abierto como de bucle cerrado. Integra el procesamiento seguro de transacciones, lo que mejora la seguridad del sistema.

El VSAM también incorpora el kernel EMV L2, optimizado para transacciones Visa "Online Deferred", y proporciona una interfaz con un lector sin contacto con certificación EMV Nivel 1 para realizar todas las transacciones EMV de forma rápida, segura y sencilla.

Esto significa que puede incorporar la tecnología de tarjetas EMV sin contacto a sistemas heredados sin modificar el software de la aplicación de validación ni el sistema administrativo del sistema de cobro automático de tarifas.

El VSAM se puede actualizar remotamente, tanto en sus tablas internas, llaves (rotación) como en su software, utilizando un método seguro para ambos. Además del kernel EMV L2, el VSAM ofrece la flexibilidad de admitir otros kernels de esquema EMV, lo que lo convierte en un producto muy potente, seguro y personalizable.

El VSAM es el núcleo del ecosistema EMV de Planeta y se integra a la perfección con el lector SCR916 y la arquitectura AIPA. Al alojar los kernels de bandera directamente en su entorno seguro, el VSAM garantiza una replicación sencilla y una alta portabilidad en diversas configuraciones de hardware. Diseñado para una máxima eficiencia, aprovecha la interfaz de alta velocidad del SCR916 para ofrecer un rendimiento de procesamiento máximo tanto para tarjetas EMV como de bucle cerrado. Su diseño no intrusivo basado en AIPA permite una operación ágil en sistemas de bucle abierto o cerrado, a la vez que admite la gestión remota completa para la carga de kernels, configuraciones y listas actualizadas.

Aplicaciones

- Sistema de pago seguro en línea y fuera de línea
- Integración EMV para transporte público

Ventajas clave

- **Ecosistema EMV integrado:** Una solución unificada y no intrusiva que combina las arquitecturas SCR916, VSAM y AIPA para operaciones fluidas de circuito abierto y cerrado.

Av. Dr. Romeu Tórtima, 272
Campinas – SP CEP 13084-791
Brazil +55 (19) 3749-8855
comercial@planeta.inf.br

- **Portabilidad certificada**: Conserva las certificaciones existentes en diferentes plataformas, simplificando drásticamente las nuevas integraciones al requerir únicamente una prueba de regresión.
- **Gestión sin intervención**: Prepara su negocio para el futuro con la carga remota completa de kernels, configuraciones y listas negras, eliminando la necesidad de intervención en campo.
- **Seguridad avanzada de circuito cerrado e híbrida**: Aloja internamente aplicaciones EMV y de circuito cerrado, lo que proporciona una seguridad superior y una migración sin esfuerzo entre diferentes medios o plataformas.
- **Alta capacidad de kernel**: Ofrece la flexibilidad de alojar aproximadamente 8 kernels independientes simultáneamente, lo que permite un panorama de pagos diverso y en constante evolución.
- **Interfaz de rendimiento optimizado**: Diseñada específicamente para aprovechar las interfaces ISO7816 de alto rendimiento, como las del SCR916, garantizando el máximo rendimiento de las transacciones. •
- **Compatible con múltiples emisores**: El SAM es perfecto para ecosistemas donde diferentes proveedores de servicios (p. ej., transporte y pagos) necesitan compartir el mismo entorno seguro.
- **A prueba de futuro**: La compatibilidad con RSA 4096 y ECC 521 garantiza que el producto cumpla con los estándares de seguridad para la próxima década.
- **Garantía EAL5+**: El hardware cuenta con seguridad de nivel gubernamental.

Capacidades

El **kernel EMV L2 del VSAM** puede manejar:

- VCTKS 1.1 (Visa Contactless Transit Kernel Specification)
- Validaciones EMV L2
- 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
- Validación FDDA
- Fecha de expiración
- Especificación Visa Ready MTT (movilidad y transporte masivo), transacciones preautorizadas y listas de denegación.
- Puede realizar validación DDA para otras marcas.
- Proporciona una interfaz con el lector sin contacto certificado EMV Nivel 1 basado en APDU (Unidad de datos de protocolo de aplicación: la unidad de comunicación entre un lector y una tarjeta) que admite todos los comandos necesarios para la aplicación de pago sin contacto EMV.
- Utiliza los conceptos de Mirror, Virtualization e Interception.
- APIs para gestionar la virtualización de MIFARE Classic sobre Cipurse, Mifare Plus y DESFire (tecnologías de tarjetas seguras).

Aplicaciones personalizadas

Soporte para la carga de aplicaciones personalizadas en el entorno seguro basado en la tecnología M^{2}ESA (patente pendiente).

Especificaciones

- **Alimentación:**
  - Estándar ISO7816
- **Dimensiones:**
  - ID-1 (85.6 x 54 mm) with ID-000 plugin (25 x 15 mm)
- **Interfaces:**
  - ISO7816
- **Temperatura de operación:**
  - -25 a 85°C

Características adicionales:

- Arquitectura de Seguridad y Confianza
  - Certificación de Hardware: Construido con hardware certificado Common Criteria (CC) EAL5+ para máxima resistencia a la manipulación.
  - Aprovisionamiento Seguro: Ofrece un método altamente seguro para

descargar claves en el SAM basado en su Clave Pública única.
    - Identidad y Trazabilidad: Cada SAM puede ser registrado por una Autoridad de Certificación (CA) con su Clave Pública y Número de Serie del Chip (CSN).
    - Compatibilidad con Múltiples Emisores: Diseñado como una entidad de confianza para facilitar aplicaciones multiemisor, permitiendo que diversos proveedores operen en la misma infraestructura de forma segura.
- Rendimiento y Eficiencia
    - Motor de Criptografía de Hardware Ultrarrápido: Aceleración de hardware dedicada para todas las operaciones criptográficas.
    - Potencia de Procesamiento: Velocidad de reloj de 50 MHz / 1 MB de Flash / 32 KBytes de RAM.
    - Velocidad Inigualable: Cifrado AES en menos de 10 µs.
    - Velocidades de transferencia de datos de hasta 1,25 Mbit/s.
    - Alimentación Versátil: Funcionamiento con doble voltaje (3 V o 5 V). • Conectividad y formatos
- Comunicación: ISO7816-3 (T=0 o T=1).
    - Formatos físicos: Disponible en ISO7810, 2FF y 3FF.
    - Compatible con aplicaciones: Compatibilidad total con aplicaciones cliente RISC-V.
- Suite criptográfica avanzada (basada en hardware)
    - Criptografía simétrica
    - Compatible con los modos ECB, CBC, CTR y GCM:
    - AES: 128, 192 y 256 bits.
    - DES/3DES: 2K3DES, 2K3DES16 y 3K3DES.
    - DUKPT: Compatibilidad nativa con DUKPT-3DES y DUKPT-AES (128/192/256).
    - Almacenamiento: Hasta 128 claves simétricas y 3 RSA por directorio.
    - Criptografía asimétrica
    - RSA: De 1024 a 4096 bits (cifrado, descifrado, firma y generación de claves en chip).
    - ECC (curva elíptica): De 112 a 521 bits (admite 26 curvas; firma, verificación y generación de claves en chip).
    - Acuerdo de claves: ECDH (secp256 y curvas configurables) y Diffie-Hellman.
    - Almacenamiento: Hasta 3 pares de claves RSA por directorio.
    - Funciones hash e integridad
    - SHA: Compatibilidad completa, desde SHA-1 hasta SHA-512.
    - Integridad: CRC de 16/32 bits y diversificación CMAC.
    - Bibliotecas certificadas: Precargadas con bibliotecas criptográficas certificadas.

Código comercial

VSAM (I0285)

Garantía

12 meses