VSAM

VSAM – Módulo de acesso seguro de virtualização

Descrição

O SAM (Secure Access Module) é um cartão inteligente de formato plug-in que aprimora a segurança e o desempenho criptográfico em terminais de pagamento, como validadores, para cartões EMV sem contato.

O VSAM (Virtualization SAM – patente pendente), como seu irmão para aplicativos de circuito fechado, o CL_SAM, estende esses recursos ao fornecer pagamentos de circuito aberto e fechado. Ele incorpora processamento de transações seguro, o que aprimora a segurança do sistema.

O VSAM também carrega o kernel EMV L2, otimizado para transações Visa “Online Deferred”, e fornece uma interface com um leitor sem contato certificado EMV Nível 1 para executar todas as transações EMV de forma rápida e segura com fácil implementação.

Isso significa que ele pode adicionar a tecnologia de cartão sem contato EMV em cima de sistemas legados sem alterar o software do aplicativo validador ou o back office do sistema de cobrança automática de tarifas.

Gerenciamento Remoto de Ciclo de Vida: O VSAM permite atualizações remotas seguras, abrangendo não apenas suas tabelas internas, mas também o software de base (firmware) e a rotação de chaves criptográficas, utilizando protocolos de segurança avançados para ambos os processos.

Além do kernel EMV L2, o VSAM tem a flexibilidade de suportar outros kernels de esquema EMV, tornando-o um produto muito poderoso, seguro e personalizável.

O VSAM é o núcleo do ecossistema EMV da Planeta, funcionando em perfeita integração com o leitor SCR916 e a arquitetura AIPA. Ao hospedar kernels de flags diretamente em seu ambiente seguro, o VSAM garante fácil replicação e alta portabilidade em diversas configurações de hardware.

Projetado para máxima eficiência, ele aproveita a interface de alta velocidade do SCR916 para fornecer desempenho de processamento máximo para cartões EMV e de circuito fechado. Seu design não intrusivo baseado em AIPA permite operação ágil em sistemas de circuito aberto ou fechado, ao mesmo tempo que oferece suporte completo ao gerenciamento remoto para o carregamento de kernels, configurações e listas atualizadas.

Aplicações

- Sistema de pagamento on-line e off-line seguro
- Integração EMV de transporte público

Principais vantagens

- **Ecossistema EMV integrado**: Uma solução unificada e não intrusiva que combina as arquiteturas SCR916, VSAM e AIPA para operações perfeitas em circuito aberto e fechado.
- **Portabilidade certificada**: Preserva as certificações existentes em diferentes plataformas, simplificando drasticamente novas integrações, exigindo apenas um teste de regressão.
- **Gerenciamento sem intervenção**: Prepara seu negócio para o futuro com o carregamento remoto completo de kernels, configurações e listas negras, eliminando a necessidade de intervenção em campo.
- S**egurança avançada em circuito fechado e híbrido**: Hospeda internamente aplicativos EMV e de circuito fechado, proporcionando segurança superior e migração descomplicada entre diferentes mídias ou plataformas.
- **Alta capacidade de kernel**: Oferece a flexibilidade de hospedar aproximadamente 8 kernels independentes simultaneamente, permitindo um cenário de pagamentos diversificado e em constante evolução.
- **Interface de desempenho otimizada**: Projetada especificamente para aproveitar as interfaces ISO7816 de alto desempenho, como as encontradas no SCR916, garantindo a máxima taxa de transferência de transações.
- **Compatível com múltiplos emissores**: O SAM é perfeito para ecossistemas onde diferentes provedores de serviços (por exemplo, transporte e pagamento) precisam compartilhar o mesmo ambiente seguro.
- **Preparado para o futuro**: O suporte a RSA 4096 e ECC 521 garante que o produto atenda aos padrões de segurança da próxima década.
- **Garantia EAL5+**: o hardware possui segurança de nível governamental.

Capacidades

O **VSAM EMV Kernel L2** pode lidar com:

- VCTKS 1.1 (Visa Contactless Transit Kernel Specification)
- Especificação VCPS (Visa Contactless Payment System) versão 2.1.3
- MasterCard 3.4
- American Express 4.1
- Discover (DPAS) 2.0
- JCB 1.6
- Interac
- Validação FDDA
- Data de expiração
- Validações EMV L2
- Especificação de transações de mobilidade e transporte de massa Visa Ready MTT, listas pré-autorizadas e de negação.
- Pode executar validação DDA para outras marcas.
- Fornece uma interface com o leitor sem contato certificado EMV Nível 1 com base em APDUs (Application Protocol Data Unit: a unidade de comunicação entre um leitor e um cartão) que suporta todos os comandos necessários para o aplicativo de pagamento sem contato EMV.
- Usa os conceitos de Espelho, Virtualização e Interceptação.
- APIs para lidar com a virtualização do Mifare Classic sobre Cipurse, Mifare Plus e DESFire (tecnologias de cartão seguro).

Aplicações personalizadas

Suporte para carregamento de aplicações personalizadas no ambiente seguro com base na tecnologia M²ESA (patente pendente).

Especificações

- **Fonte de alimentação**: Padrão ISO7816
- **Dimensões**: ID-1 (85,6 x 54 mm) com plugin ID-000 (25x15 mm)
- **Interfaces**: ISO7816
- **Temperatura operacional**: -25 a 85 °C

Outras características:

- Arquitetura de Segurança e Confiança
  - Certificação de Hardware: Construído com hardware certificado Common Criteria (CC) EAL5+ para máxima resistência a adulterações.
  - Provisionamento Seguro: Apresenta um método altamente seguro para baixar chaves para o SAM com base em sua Chave Pública exclusiva.
  - Identidade e Rastreabilidade: Cada SAM pode ser registrado por uma Autoridade Certificadora (CA) com sua Chave Pública e Número de Série do Chip (CSN).
  - Suporte a Múltiplos Emissores: Projetado como uma entidade confiável para facilitar aplicativos com múltiplos emissores, permitindo que diversos provedores operem na mesma infraestrutura com segurança.
- Desempenho e Eficiência
  - Motor Criptográfico de Hardware Ultrarrápido: Aceleração de hardware dedicada para todas as operações criptográficas.
  - Poder de Processamento: Velocidade de clock de 50 MHz / 1MByte de Flash / 32KBytes de RAM.
  - Velocidade Inigualável: Criptografia AES em menos de 10 µs.
  - Taxas de transferência de dados de até 1,25Mbit/s.
  - Alimentação versátil: Operação com dupla voltagem (3V ou 5V).
- Conectividade e formatos
  - Comunicação: ISO7816-3 (T=0 ou T=1).
  - Formatos físicos: Disponível nos formatos ISO7810, 2FF e 3FF.
  - Pronto para aplicações: Suporte completo para aplicações cliente RISC-V.
- Conjunto avançado de criptografia (baseado em hardware)
  - Criptografia simétrica
  - Suporta os modos ECB, CBC, CTR e GCM
  - AES: 128, 192 e 256 bits.
  - DES / 3DES: 2K3DES, 2K3DES16 e 3K3DES.
  - DUKPT: Suporte nativo para DUKPT-3DES e DUKPT-AES (128/192/256).
  - Armazenamento: Até 128 chaves simétricas e 3 RSA por diretório.
  - Criptografia assimétrica
  - RSA: 1024 a 4096 bits (Criptografia, Descriptografia, Assinatura e Geração de Chaves On-chip).
  - ECC (Curva Elíptica): 112 a 521 bits (Suporta 26 curvas; Assinatura, Verificação e Geração de Chaves On-chip).
  - Acordo de Chaves: ECDH (secp256 e curvas configuráveis) e Diffie-Hellman.
  - Armazenamento: Até 3 pares de chaves RSA por diretório.
  - Funções de Hash e Integridade
  - SHA: Suporte completo de SHA-1 a SHA-512.
  - Integridade: Diversificação CRC de 16/32 bits e CMAC.
  - Bibliotecas Certificadas: Pré-carregadas com bibliotecas criptográficas certificadas.

Código comercial

VSAM (I0285)

Garantia

12 meses.