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), 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.

O VSAM é atualizável remotamente, não em suas tabelas internas, mas também em seu software, usando um método seguro para ambos.

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

Garantia

6 meses

Código comercial

- VSAM (I0285)

Aplicações

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

Capacidades

O VSAM EMV Kernel L2 pode lidar com:

- Validação FDDA
- Data de expiração
- Validações EMV L2

- Especificação VCPS (Visa Contactless Payment System) versão 2.1.3
- 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 APDUsv (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).

Especificações

- **Fonte de alimentação:**
  Padrão ISO7816
- **Dimensões:**
  ID-1 (85,6 x 54 mm) com plugin ID-000 (25 x 15 mm)
- **Interfaces:**
  ISO7816
- **Temperatura operacional:**
  0 a 70°C
- **Outras características:**
- Hardware com certificação CC EAL5+.
- Mecanismo de criptografia de hardware ultrarrápido.
- Maneira segura de baixar chaves no SAM com base em sua chave pública.
- Cada SAM pode ser registrado por uma Autoridade Certificadora com uma cópia de sua chave pública e CSN. A CA pode ser uma entidade confiável para dar suporte a um aplicativo multe emissor.