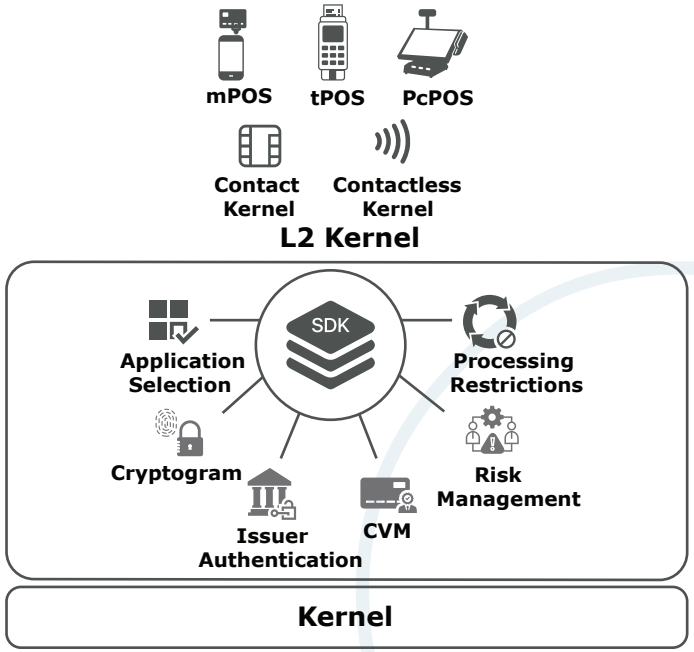
Kernel



EMV L2 Kernel enables a card acceptance on smart phones to process EMV transactions, Enables Smart phone or POS application to support EMV transactions from various payment schemes and closed loop.
Security review by assigned labs
Library is fully compliant with the EMV standard specifications and interfaces with WBC for cryptographic operations and key management.
TMS enables to manage the controlling the kernel entry points and parameters.

Benefits

- EMV Compliance
- Fast development
- Fast time to market
- Functional Evaluation Ready
- Highly Portable to different platforms
- Completely controlled by parameters & TMS
- Security Module for independent evaluation and porting

Kernel Features

- Application Selection
- Final Selection
- Get processing options
- READ RECORD Command-Response APDUs
- Processing Restrictions
- Cardholder Verification & CVM Processing Logic
- Terminal Risk Management (Floor Limits,
- Random Transaction Selection, Velocity Checking) GET DATA Command-Response
- APDUs VERIFY Command-Response APDUs
- GENERATE AC
- Data Authentication (SDA/DDA/CDA) Combined DDA Application
- Cryptogram Generation (CDA)
- Kernel DB
- Diagnostic report
- Online result processing
- Issuer script processing

Parameter functions

- GetParameters
- GetTag
- UpdateTag

Platform features

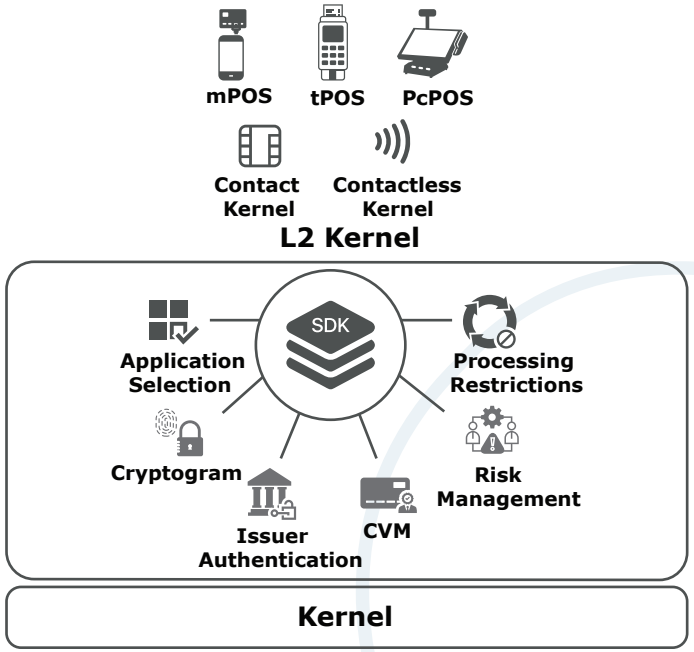
- Technology - C/C++, JNI
- Code Size - ~25k lines source
- EMV Standard - EMV Level 2
- Platform - Mobile, PC, Any 32 bit platform
- Required Libraries - Open SSL, - SHA-1, RSA, SHA-1
- Configuration - Fully configurable from TMS
- Easy to integrate APIs

Kernel APIs

- Application Selection
- Initiate App Processing
- Read Application
- Offline Authentication
- Process Restrictions
- Card Holder Verification
- Terminal Risk Management
- Terminal Card Action Analysis
- Host Processing

Call-back APIs

- Clear Display
- Display
- Random Number
- FetchCAPK
- SelectApp
- Amount Entry
- PIN Entry



EMV L2 Kernel enables a card acceptance on smart phones to process EMV transactions, Enables Smart phone or POS application to support EMV transactions from various payment schemes and closed loop.
Security review by assigned labs
Library is fully compliant with the EMV standard specifications and interfaces with WBC for cryptographic operations and key management.
TMS enables to manage the controlling the kernel entry points and parameters.

Kernel Configurations

- Configurable data authentication - DDA, SDA, CDA, fDDA
- Configurable CVM (Mobile, Online, Offline, Signature)
- Configuration of limits - Amount, Floor limit, CVM limit

Pre-Certification

- EMVCo Type Approval Terminal Level 2 Test
- Cases execution
- Capture L2 Traces
- Report Generation
- Security review by assigned labs

L2 Certification

- EmvCo Registration
- Submit the ICS form
- Get the Test cases from EmvCo
- Run the test cases at assigned lab
- Submission test results for L2 Kernel
- Feedback correction and re-submit Security
- Security Review at assigned lab

L3 Certification

- Acquirer certification with Card schemes
- (Visa ADVT, CDET, VPTT, MC MTIP, Pay Pass, Amex, RuPay etc.)
- Register with the Card scheme
- Get the ICS form filled and submit Execute
- the L3 scripts received using UL tool

Performance of the Platform

- Code coverage >90%
- Duplication < 7%
- Extended logging across platform - 100%
- Automation coverage >90%Performance -
- As acceptable by Schemes