NEWNET DATA SHEET

TransKrypt Security Server

Overview

Security of transactions is critical as the volume of payments are growing at a faster pace from new generation mobile and broadband based IP payment terminals and devices. NewNet's TransKrypt Security Server is a comprehensive security server solution aimed at offering multiple security solutions which are crucial to payment transaction processing.

TransKrypt offers both virtualized operations and datacenter server options, with the TransKrypt Cloud Edition as part of Secure Transaction Cloud (STC) and the TransKrypt Server Edition respectively.

TransKrypt Security Server offers the following security functions:

- Point to Point Encryption (P2PE)
- Tokenization

The solution offers Point to Point Encryption(P2PE) for supporting data encryption from POS/POI terminals, and Tokenization of card and sensitive data for payment transactions.

Secure cryptographic devices used for cryptographic-key management functions and/or the decryption of account data are host/hardware security modules (HSMs), which are approved and configured to FIPS140-2 (levels 2 & 3).

TransKrypt Point To Point Encryption (P2PE) System

TransKrypt Security Server offers the P2PE solution for Acquirers/Processors and Service Providers working in conjunction with approved point of interaction devices that are certified for usage in a P2PE environment. The P2PE solution supported by NewNet's TransKrypt Security Server is based on ANSI X9.24 standards specified DUKPT mechanisms.

NewNet's TransKrypt Security Server utilizes FIPS 140-2 Level 2 HSM solution to store sensitive data like encryption keys securely and provide encryption and decryption capabilities. TransKrypt Security Server solution provides P2PE capability for Terminal Line Encryption using Derived Unique Key Per Transaction (DUKPT) working in conjunction with the NewNet AccessGuard and Total Control STG systems which aggregates, switches and routes transaction from POS devices.

TransKrypt Tokenization System

TransKrypt Security Server system offers Tokenization solution for Acquirers/Processors and Service Providers with standards based token issuance solution with the capability of de-tokenization as well. Tokenization is a process by which the primary account number (PAN) or other sensitive data is replaced with a surrogate value called a token. Detokenization is the reverse process of redeeming a token for its associated PAN value. The tokenizer application provides an interface for tokenizing the input data string into desired length. Similarly the token can be converted back to the original data as required.

Tokenization solution uses HSM module which is a tamper proof device to store keys used for the tokenization. The HSM module ensures that the encryption keys and sensitive data reside on a secure device and cannot be accessed or tampered with without destroying the module. The tokenization solution need to be installed in a secure location and will interface with other authorized systems using TLS/SSL with valid certificates.
Merchants can use the tokenization solution to reduce the PCI-DSS scope by storing transaction reference data with a token instead of the PAN, as recommended by PCI.

NewNet
SECURE PAYMENT TRANSACTIONS

Technical Specifications

Hardware Chassis

- 2U Rack Mount Server
- Dimensions:
  - Height: 3.44”
  - Width: 17.54” (Standard 19” rack mountable)
  - Depth: 29.5”
- Low profile (2.1” x 6.6”) PCIe form factor HSM

Security Softwares

- OpenSSL and TurboSSL
- PKCS#11 Crypto
- OpenSSH

Hardware Security Module

- Highest Performing FIPS 140-2 Hardware Security Module (HSM)
- Adapter Family
- SSL / TLS performance
  - Up to 45K 1024-bit key RSA operations / sec
- USB port for two-factor authentication
- Accelerates SSL cryptographic functions bulk Encryption
- 256-bit AES based key encrypt
  - Advanced ECC is used for handshake
- Enhanced on card storage
  - Up to 4096 concurrent server private key

Tokenization Functions

- Token issuance to POS/POI/Mobile Wallet Devices
- Detokenization for Authorized systems
- Multiple tokenization algorithms
  - Random: Generate token with random numeric string of same length
  - Hash: Generate SHA256 hash using random salt
- Token usage modes
  - Single use
  - Multiple use
  - Non-reversible token
- Device Authorization
  - Client certificate validation
  - Client authorization for access to specific APIs
- Device Interface & Access
  - IP/TLS/HTTPS POS interface for tokenization
  - HTTPS/TLS Host interface
- Validity period for retention
- Secure data vault for storage

Security Storage

- Physical and logical Cryptographic boundaries
  - Secure and tamper evident enclosure
  - All keys are secured within cryptographic boundary
- API libraries for Card and key management

Physical Interfaces

- WAN/LAN: RJ-45 (4 ports of 10/100/1000 Mbps)
- Optional 2 ports of 1/10Gbps

Operating Requirements

- 100-120 VAC, 200-240 VAC
- Max power consumption: 526W @100 VAC
- Nominal operating range:
  - Temperature: 10 to 35°C
  - Humidity: 10% to 90%
- Non-nominal operating range:
  - Temperature: -30 to -60°C
  - Humidity: 5% to 95%
- Shipping Conditions: -40 to 60°C
  - Humidity: 5% to 95%
- Shipping Conditions: -40 to 60°C

P2PE Functions

- FIPS 140-2 secure key generation
- Generate multiple Base Derivation Keys (BDK)
- Generate IPEK based on BDK
- Redundancy with a standby Server and HSM cloning
- PCI Standards compliant
- Integrated Server HW, HSM HW and Application SW
- BDK generation or upload per Acquirer/ Merchant ID
- IPEK generation based on Acquirer/Merchant ID

NewNet
SECURE PAYMENT TRANSACTIONS

