NEWNET PRODUCT BRIEF

TransKrypt Security Server

Overview

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 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.

P2P Encryption from POS to AccessGuard/Total Control STG

In a generic scenario, the transaction request from POS terminal to payment processing gateway needs to be encrypted. The following steps are part of this process to ensure the transaction is encrypted from the POS and further send securely to the payment switching and routing systems to further forward these transactions securely to the authorization servers.

Encryption Algorithm

3DES or AES crypto algorithm is used for encryption. Each transaction will have unique key to encrypt transaction requests and responses.

TRANSKRYPT

Key Generation

Key generation is based on DUKPT standards as specified by ANSI X9.24. Base keys are generated and stored in the TransKrypt Security Server within the HSM and the initial keys are securely delivered through Public Key Infrastructure (PKI) procedures directly or through the Terminal Management Systems (TMS) to the POS devices towards generating the unique keys for each transaction.

Keys for Encryption at POS

Keys are generated dynamically with each transaction and cryptographically changed to the key for the next transaction. POS terminal, while doing the current transaction, will generate the next one and store it.

Keys for Decryption at AG/STG

AG/STG interfaces with the TransKrypt Security Server which has the base key of all the super-secret key. When the POS sends the encrypted payload it also sends meta data including terminal identifier and transaction counter. With the meta-data and the super-secret key in the TransKrypt Security Server, AG/STG systems would cryptographically generate the same key that terminal used for the encryption.

Standards Compliance

Compliant to the PCI Security standards for P2PE systems for the process of decrypting the transaction data and generation and storage mechanism for the keys used for obtaining the unique keys per transaction.

Derived Unique Key Per Transaction (DUKPT)

Derived Unique Key Per Transaction (DUKPT) is a key management scheme in which for every transaction, a unique key is used which is derived from a fixed key.

Hardware Security Module (HSM)

TransKrypt Security Server uses FIPS HSM PCI-e card to generate & store keys secure.

Derived Unique Key Per Transaction (DUKPT)

Derived Unique Key Per Transaction (DUKPT) is a key management scheme in which for every transaction, a unique key is used which is derived from a fixed key.

Hardware Security Module (HSM)

TransKrypt Security Server uses FIPS HSM PCI-e card to generate & store keys secure.

Full Payload or Sensitive Field Encryption

TransKrypt Security Server’s P2PE solution offers options to select from the possible usage of entire transaction data being encrypted or only selected fields being encrypted. This allows flexibility for Acquirers, Processors and Service providers to work the POS device SW to handle encryption processes in a convenient manner as supported on the client devices.

Integrated Bi-Directional Solution

TransKrypt Security Server solution works together with the AccessGuard and Total Control STG systems to offer a full-fledged P2PE solution allowing the transport and routing of encrypted data from the POS to the Authorization Host. The traffic in the reverse direction for the authorization response from the Host server to the POS terminal is also encrypted thereby leaving no part of transaction to be left un-encrypted.

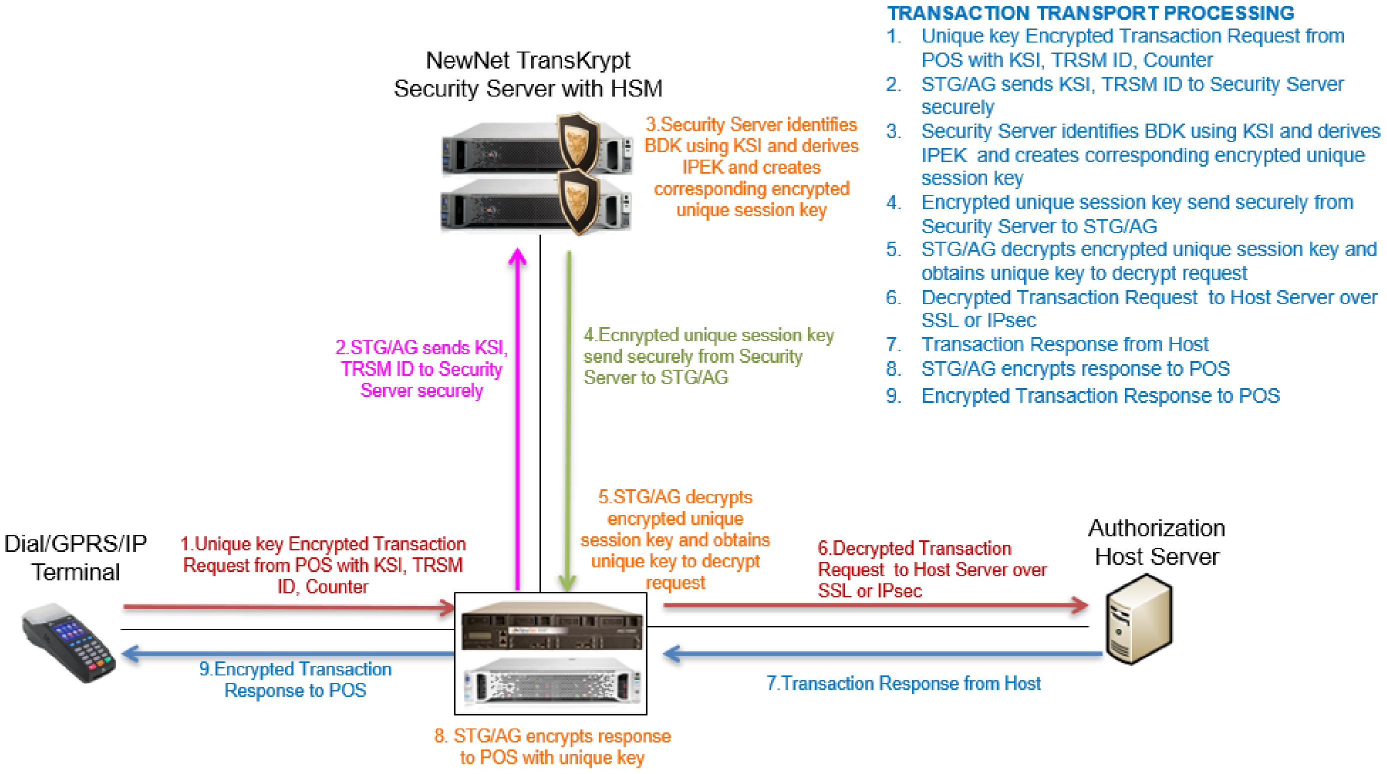
Key System Benefits

- FIPS 140-2 secure key generation server
- Generate multiple Base Derivation Keys (BDK)
- Generate Initial Phase Encryption Key (IPEK) based on 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
- Future support of Certificate Authority application and Tokenization

P2PE Benefits

- BDK generation or upload per Acquirer/Merchant ID
- IPEK generation based on Acquirer/Merchant ID
- Storage of up to 4096 keys in HSM
- Redundancy using Dual TransKrypt Security Server
- Support 7500 RSA operations/sec and 50K concurrent sessions
- Oracle Berkeley DB for internal storage

Message and Event Flow for Transaction Processing with TransKrypt


NewNet TransKrypt
Security Server with HSM
3.Security Server identifies BDK using KSI and derives IPEK and creates corresponding encrypted unique session key
2.STG/AG sends KSI, TRSM ID to Security Server securely
4.Ecnrypted unique session key send securely from Security Server to STG/AG
5.STG/AG decrypts encrypted unique session key and obtains unique key to decrypt request
Dial/GPRS/IP Terminal
1.Unique key Encrypted Transaction Request from POS with KSI, TRSM ID, Counter
9.Encrypted Transaction Response to POS
8. STG/AG encrypts response to POS with unique key
6.Decrypted Transaction Request to Host Server over SSL or IPsec
7.Transaction Response from Host
Authorization Host Server

TRANSACTION TRANSPORT PROCESSING

1. Unique key Encrypted Transaction Request from POS with KSI, TRSM ID, Counter
2. STG/AG sends KSI, TRSM ID to Security Server securely
3. Security Server identifies BDK using KSI and derives IPEK and creates corresponding encrypted unique session key
4. Encrypted unique session key send securely from Security Server to STG/AG
5. STG/AG decrypts encrypted unique session key and obtains unique key to decrypt request
6. Decrypted Transaction Request to Host Server over SSL or IPsec
7. Transaction Response from Host
8. STG/AG encrypts response to POS
9. Encrypted Transaction Response to POS

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.

The application that needs to generate a token will use the corresponding modules of the Tokenization solution and are accessed by external systems over HTTPS/TLS. The application will be authenticated using the SSL certificate and credentials provided. The credentials can be used to decide the validity of the requestor and the requestor is authorized for using the application. For the POS to generate token, the POS will send a P2PE secured and specially formatted request with suitable information along with the PAN and other details like terminal ID, merchant ID and acquirer ID to AG1000/STG systems over a TLS/SSL connection. This interface will only provide a tokenization option and the device will be validated using the POS SSL certificate and the other details provided. Detokenization is permitted to authorized devices like payment Host servers to perform with similar high security and enhanced authorization procedure.

Tokenization Functions

Tokenization application on TransKrypt Security server represents a cutting edge FIPS 140-2 Level 3 Certified HSM based high security solution targeting the payment, financial sectors for ensuring tokenized payments to enhance security of transactions.

The key features of the solution are listed below.

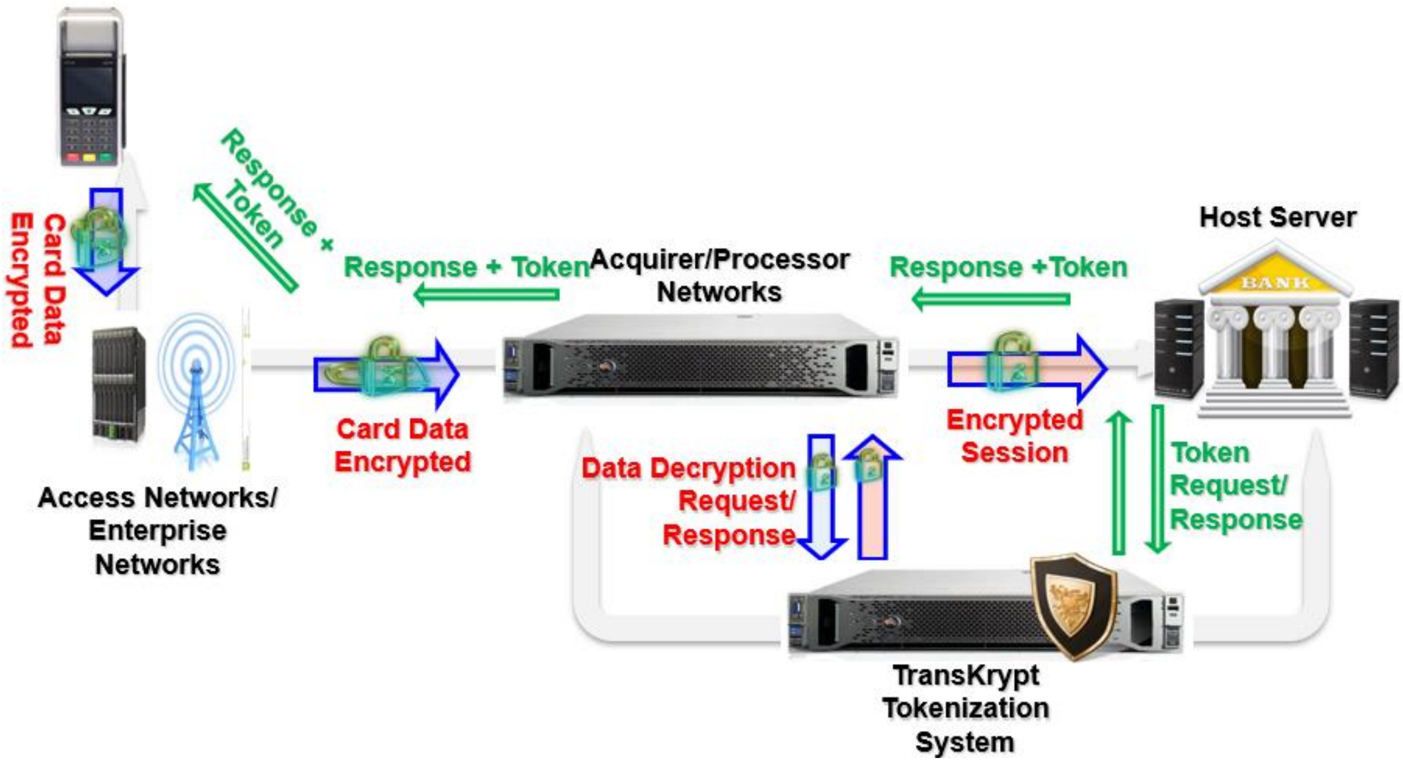
- Replace sensitive data with random one time uniquely identifying Tokens
- Token issuance to POS/POI/Mobile Wallet Devices
- Detokenization for Authorized systems
- Multiple tokenization algorithms
  - Random – generate token with random numeric string of same length
  - Hash – generate SHA256 hash 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

Key Tokenization Operations

All tokenizer operations are exposed over the HTTPs interface. The application needs to provide a valid client SSL certificate and also the credentials for authentication and authorization. The credentials are passed in the HTTP header.

1. **Creating a Card Data Vault:** The card data vault (CDV) can be created by a user with admin role.
2. **List Card Data Vaults:** The CDVs available can be retrieved by a user with admin role.
3. **Generate Token:** A token can be generated by user with tokenizer role.
4. **De-tokenization:** The PAN or original data can be retrieved based on a token by a user with privileged role.
5. **List Token Handles:** List of token handles that expire in a time interval can be retrieved by a user with privileged role.

- No concerns for merchant on storage and security of customer card data
- Validate systems to conform with PCI standards
- Ensure back end systems are compliant with PCI requirements
- Limits PCI scope, reduces merchant vulnerability, improves payment security



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

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