

# Secure Transaction Cloud (STC)

## Virtualized Secure Cloud Payment Routing & Transport Solution



**SECURE  
TRANSACTIONS  
CLOUD**

### Highly Secure

Uses Cloud based HSM high security crypto engine.

### Fast “Time-to-Market”

Installation in minutes with capacity expandable via feature key enabling procedure.

### Lower Cost of Ownership

Standards-based system delivers high transaction density in cloud infrastructure with lowest cost.

### Investment Protection

Minimal to no modifications required to existing hosts and fully compatibility to existing host application protocols and can be used with existing POS terminals.

### Industry Protocol Support

Supports latest standards such as Visa I, Visa II, TPDU, ISO8583, ISO20022; security with TLS 1.2, P2PE, Tokenization.

### Highly Versatile

Integrates TLS processing, protocol-based routing, transaction processing, IP network routing, redundancy, management and reporting on a single instance of the application in cloud.

## Cloud for Payment Transactions

As Cloud adoption increases, Payment Acquirers, Processors, FinTechs, ISOs, Mobile Operators and Payment Service Providers expect a secure, reliable and performance driven payment transaction solution that fits their cloud migration strategy.

NewNet helps build a fully cloud-native payments solution by a cloud-based payment transport and acquiring application for public cloud or private cloud infrastructure, with AWS CloudHSM, Google Cloud HSM etc or FIPS certified hardware security module in private cloud or virtual environments, that delivers a high-volume, low-latency payment processing.

## Secure Transaction Cloud (STC) Payment Routing Solution

Software as a Service (SaaS) model is the common model available for payment transaction handling with the capability provided to the acquirer, processor and merchant transaction processing entities to use the payment and security applications running on a cloud infrastructure. NewNet’s Secure Transaction Cloud (STC) offers AccessGuard Cloud Edition and TransKrypt Cloud Edition applications.

These application are accessible from various client devices through either a thin client interface, such as a web browser, or a suitable application program interface. The end customer is transparent to the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities. The acquirers/processers availing the service only manage the limited user-specific application configuration settings.

## STC Virtualized Secure Payment Applications

NewNet’s Secure Transaction Cloud Solutions offer NFV based virtualized secure payment applications of AccessGuard Cloud edition and TransKrypt Cloud Edition with a broad range of Virtual Networks Functions (VNF) including:

- TLS, IPsec, SSH, and HTTPS for added Security
- ISO8583, TPDU, VISA, ISO2022(XML) Transaction Protocols
- Tokenization and P2PE
- Host Interfaces
- Load Balancing

## STC Virtualized Capabilities

These virtualized capabilities allow the solution to support the full plethora of payments including internet payments, mobile payments, POS based transactions which are IP/Mobile access based and all forms of ecommerce and mcommerce payments with PCI standards compliant security. With virtualized payment and security functions operating in the cloud infrastructure along with cloud HSMs, the security of the solutions remains the highest as stipulated by the standards bodies, with the strongest encryptions using long length keys, and crypto operations being handled completely within the HSM boundaries. REST/JSON which follow the SOA model and used by web service-based software architectures are used for integration purposes of the NST payment application with cloud services and also for service orchestration.

## STC - AccessGuard Cloud Edition Feature Specification

### IP Protocols

- NTP
- TCP/IP
- DNS
- LDAP
- RIPv2
- HTTP

### Management

- SNMP
- SSH
- GUI
- Alarms/Traps
- Syslog

### Transaction Protocol Support

- Transparent
- VISA I/II (EIS)
- ISO 8583
- TDPU
- ISO 20022(XML)

### Security

- TLS v1.2
- PCI Security Requirements
- Digital Certification
- DUKPT

### MACS

- SHA256
- SHA384
- MD5
- SHA1

### Certificate Key Length

- RSA 2048 bits
- RSA 4096 bits

### Key Exchange

- RSA
- Diffie-Hellman

### Encryption

- AES (192,256)
- 3DES (168)
- RC4 (128)

## STC - TransKrypt Cloud Edition Feature Specifications

### Security Softwares

- OpenSSL and TurboSSL
- PKCS#11 Crypto
- OpenSSH

### Security Functions

- Key management
- PKI
- Authentication
- Application level encryption
- File security
- Digital signatures

### P2PE & Tokenization Security Functions

- 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
- Tokenization & Detokenization

### Security Storage

- Logical cryptographic boundaries
- All keys are secured within cryptographic boundary
- Cloud HSM
- API libraries for card and key management

