Secure Transaction Cloud (Standard)

Virtualized secure cloud payment routing

Why Secure Transaction Cloud?

- Highly secure: Uses cloud-based hardware security module (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 full compatibility to existing host application protocols and point of sale (POS) terminals.

Product overview

The Secure Transaction Cloud (STC) solutions offer network functions virtualization (NFV) based virtualized secure payment applications for transaction transport, routing, and switching. This comes with specific virtual network functions (VNF) for security, transaction protocols, tokenization, host interfaces, load balancing, etc. The virtualized capabilities allow the solution to support a wide range of payment types. These include internet payments, mobile payments, and point of sale (POS) based transactions which are internet protocol (IP) and mobile access based. Also supported are ATM transactions and all forms of eCommerce and mCommerce payments with payment card industry (PCI) standards compliant security.

Product features

TLS acceleration
Transport layer security (TLS) acceleration is a method of offloading the processor-intensive public key encryption algorithms involved in TLS transactions to a hardware accelerator. The TLS Accelerator solves the problem of server (host) slowdowns caused by running TLS in software using the host central processing unit (CPU).

Key exchange algorithm
Symmetric key cipher requires a key to be used to encrypt the communications. When two parties have no prior knowledge of each other, they must jointly establish a shared secret key for encryption over an insecure communications channel.

Digital certificate
Key agreement or key transport schemes are vulnerable to man-in-the-middle attacks. A solution to this problem is to send the public key over the communication link using a signed certificate. A certificate contains, along with the public key of the sender, the name of the certificate holder. It also contains the digital signature of an independent and trusted third party, called certification authority (CA), to ensure the validity of the transmitted information.
How it works

Security is handled exclusively within the cloud-based hardware security module (HSM) with partitions for virtual instances, and this is most critical to concentrate all crypto operations within the HSM. The platform offers the capability to handle TLS with point-to-point encryption (P2PE), TLS with tokens, and more within a single step process. Enabling encryptions between the multiple protocol handoffs facilitates the complex goal of no software application having any access to any of the crypto operations. This protects the solution from a chance of data compromises via any malware issues trying to scum the application memory space.

The security procedures followed are compliant to the multiple PCI requirements which attributes to the handling of HSM, secure sessions, tokens, virtualization, etc. The solutions are compliant to the payment card industry data security standard (PCI DSS) 3.2, PCI P2PE 2.0, PCI Tokenization Guidelines, and PCI DSS Virtualization Guidelines. The HSM system used for the solution is certified with FIPS 140-2 Level 3 and conforms to the highest levels of security requirements for the storage and security of key and cryptographic operations.

Differentiators

- Enables reliable and scalable transaction transport, switching, and routing systems for fast transaction processing of credit card authorization.
- Provides decryption of encrypted data from payment devices, certificate verification of client POS devices, and tokenization of card holder data.
- Integrates TLS processing, protocol-based routing, transaction processing, IP network routing, redundancy, management, and reporting on a single instance of the cloud.
Data Points

- 4096 Keys stored in HSM storage
- 726B+ Global electronic payments in 2020

Additional Resources

- NewNet datasheets
- STC solution
- STC datasheet

Solution available in AWS Marketplace