NEWNET PRODUCT BRIEF

Secure Transaction Cloud (STC)

Virtualized Secure Cloud Payment Acquiring & Transport Solution

Cloud for Payment Transactions

Cloud adoption by service providers and enterprises is expected to advance rapidly through 2020. As the cloud adoption extends to all industries, payment, financial and banking sectors are also making the migration to public, private or hybrid cloud models. In this fast- changing cloud bound world, payment providers require a high security, reliability and performance delivering payment transaction solution to fit into their cloud migration strategy, and NewNet offers a proven virtualized payment application to meet this demand.

Cloud computing for payment handling enables on-demand network access to a shared pool of computing resources including networks, servers, storage, applications etc. that can be rapidly provisioned and availed with minimal management effort or service provider interaction, to facilitate payment transaction handling. Key characteristics of cloud services include on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. Of the three service models possible with cloud services comprising Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS); these services may be deployed as private cloud, public cloud, hybrid cloud and community cloud.

Private cloud for payment handling has the cloud infrastructure provisioned for exclusive use by a single organization like an acquirer/processor/MNO comprising multiple consumers which may be owned, managed, and operated by the organization, a third party, or some combination of them. This may exist on or off premises of the respective enterprises or Carriers and MNOs. Public cloud which is quite popular with the newer generation payment solutions and services has the cloud infrastructure provisioned for open use by the general public. This is mostly owned and operated by a business, academic, or government organization, or a combination of these. It exists on the premises of the major cloud providers.

Hybrid cloud infrastructure holds potential benefits with payment handling with two or more distinct cloud infrastructures (private or public) that remain unique entities, but are bound together by suitable interface mechanism for application and data portability. This model facilitates the extensions of the payment data handling from the private cloud to the public cloud environments as well.

According to Gartner, Inc. worldwide public cloud services market is projected to grow over 16% in 2016 to total $204 billion. Cloud application services (SaaS) is forecast to grow over 20% percent in 2016, to $37.7 billion. This holds huge potential in enabling faster service rollout for green field entrants and those existing players looking for rapid migration from data center environments to cloud based solutions.

Secure Transaction Cloud (STC) Payment Acquiring 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. The applications 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/processors availing the service only manage the limited user-specific application configuration settings.

Cloud providers offer the payment Platform as a Service (PaaS) as well wherein the capability is provided to deploy onto the cloud infrastructure payment transaction and financial technology application of vendors like NST created using services, and tools supported by the cloud service provider. The end customers are typically the acquirers, payment service providers or transactions service providers, and they can worry less about managing the underlying cloud infrastructure including network, servers, operating systems, or storage. They only manage the deployed applications and possibly configuration settings for the application-hosting environment.

STC Virtualized Secure Payment Applications

NewNet's Secure Transction Cloud solutions offer NFV based virtualized secure payment applications with a broad range of Virtual Networks Functions (VNF) including:

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

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 based HSM, 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.

Transaction Flows with STC

Cloud based payment solutions from NST enables the options for client payment devices (POS/POI terminals, smart payment devices etc.) to alleviate them for any security concerns with the capability to handle all sensitive information from the cloud infrastructure based on an on-demand model and thus leaving the client payment devices at no risk of any storage of sensitive information. The sensitive information including all Keys, PINs, Card data etc. which otherwise may get retained within the payment devices or the applications associated with retail merchant transaction systems.

Client payment terminals originate the transactions as normal payment transactions and these are securely routed to the cloud infrastructure which may be private cloud of the acquirer/processor or public clouds which may be offering the services for the acquirers/processors. The NST cloud based payment solutions present in the respective cloud environment handles these transactions in high security zone with cloud based HSM and perform the protocols routing, P2PE handling, Tokenization as needed and securely passes these to the Authorization servers. In the response direction as well the transactions are securely handled back from the Authorization servers through the cloud infrastructure and back to the payment terminals.

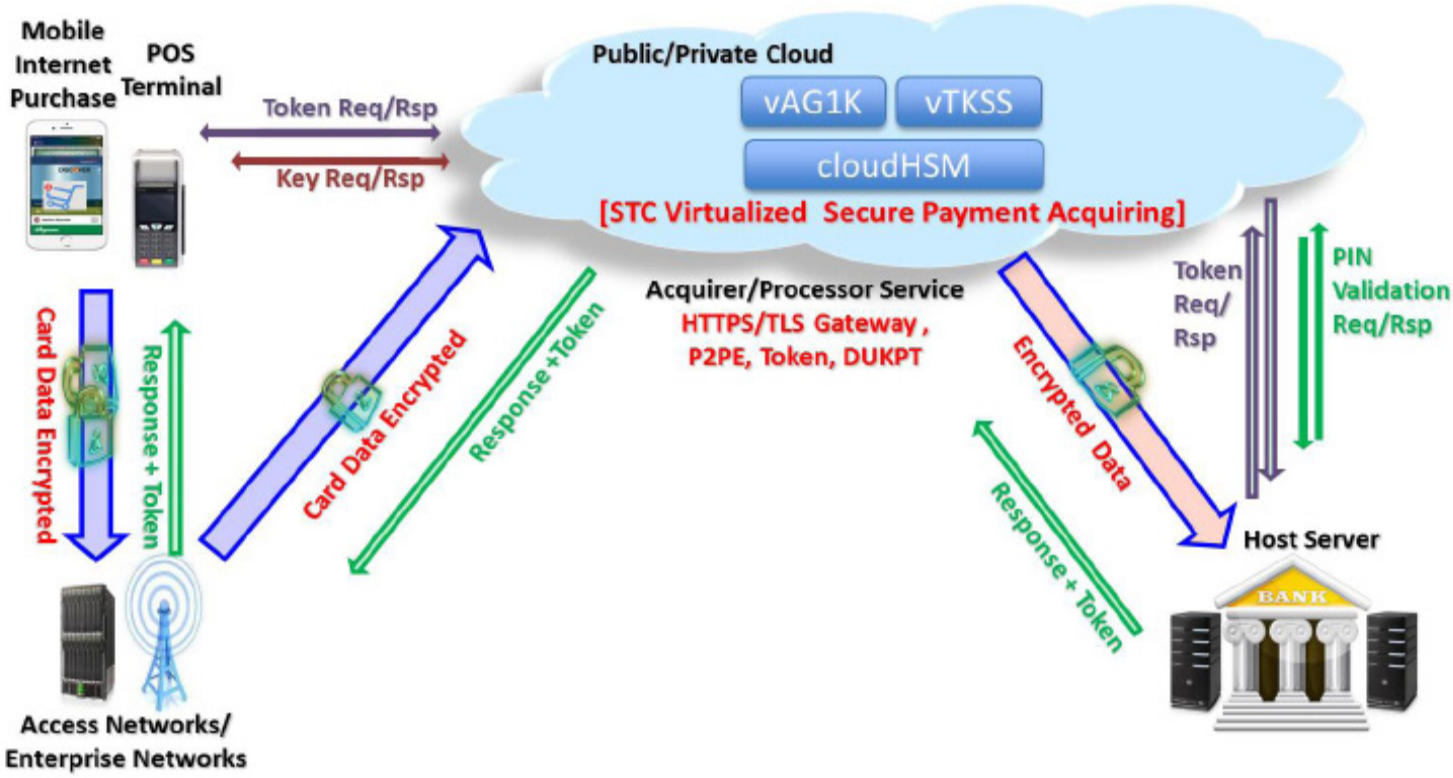
Sessions are connected with TLS/HTTPS for security and the card data is encrypted with P2PE. Tokenization replace the sensitive card data and the tokens are retained with merchant systems, which ensure full compliance to the PCI standards and limits the scope of the PCI requirements of the merchants to the maximum extent.

Security & Key Management

Security is handled exclusively within the cloud based HSM with partitions for virtual instances, and this is most critical to concentrate all crypto operations within the HSM. The capability to handle TLS with P2PE, TLS with Tokens etc. within a single step process and having encryptions established 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 any chances of data compromises via any malware attacks trying to scrum 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 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.

STC Virtualized Transaction Solution for Cloud Based Payments



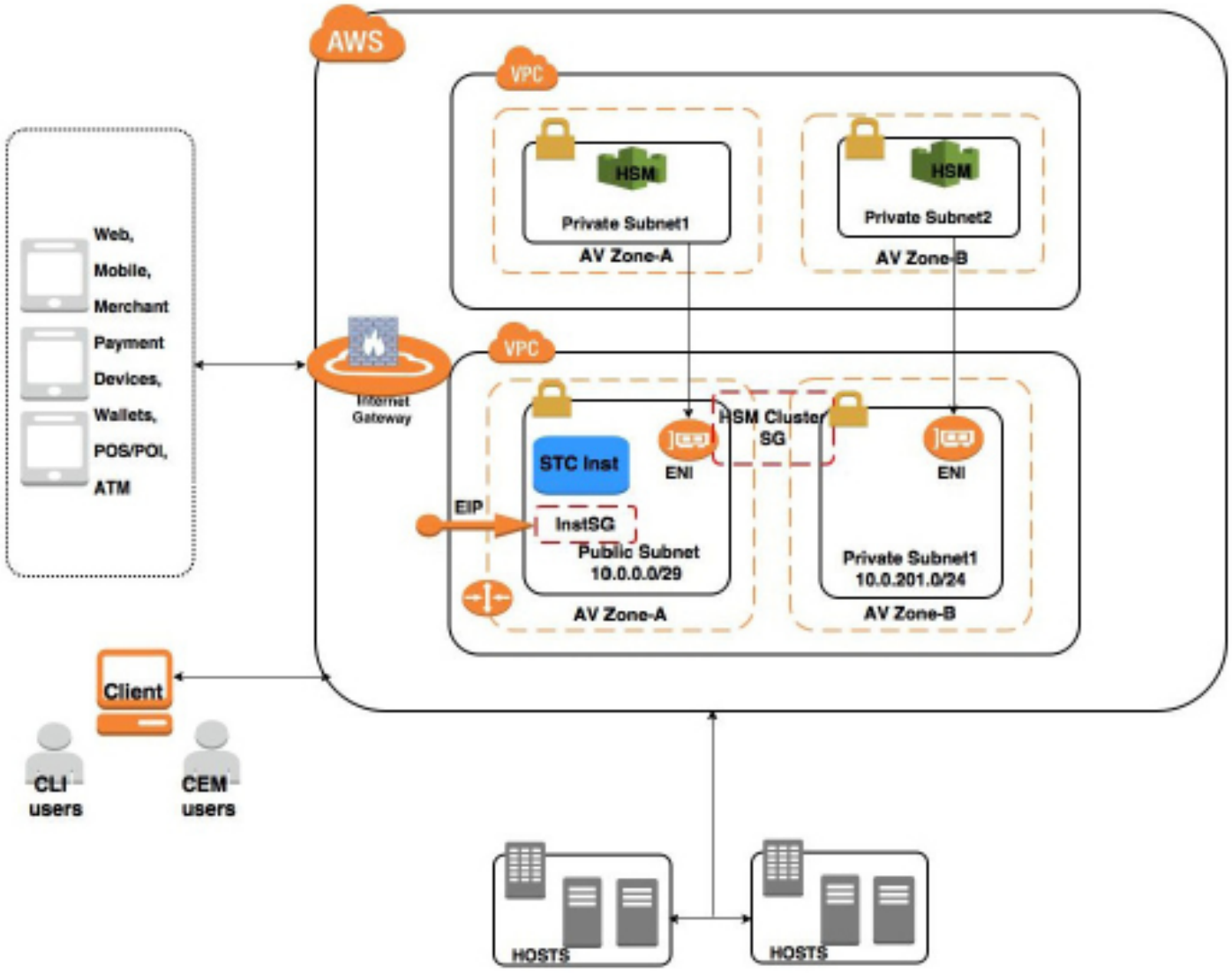
STC Benefits

STC virtualized payment transaction solutions for cloud services can be operated in a public, private or hybrid cloud infrastructure and offers a wide range of benefits for the acquirer/processor or MNO/Carrier customers. These benefits are attributed to multiple advantages that this solution offers including the key intellectual knowhow in payments, networking and virtualization being extended to the cloud based solutions along with the comprehensive embedding of the virtualized application solutions in the cloud providers' infrastructure.

The solution offers the benefits of NFV and SDN capabilities ensuring the handling of high volume traffic with rapid ease of scaling and limited time to market.

- HSM based security with FIPS certified boundaries controlling the entire crypto operations
- Service available over the network and accessed through standard mechanisms
- Supports heterogeneous thin or thick clients on POS/POI Devices, smart phones, web applications
- Computing resources are pooled to serve multiple users
- Physical, virtual resources dynamically assigned and reassigned as per demand
- Rapid elasticity for services to be elastically provisioned and released
- Automatically control and optimize resource use by metering
- Resource usage is monitored, controlled, and reported
- Transparency for customers on details of the utilized service
- Support of public, private, hybrid cloud solution models

STC Payment Application in AWS Cloud Infrastructure



STC - AccessGuard Cloud Edition

STC's AccessGuard Cloud Edition from NewNet is designed to securely route millions of mobile, broadband IP based payment transactions. AccessGuard Cloud Edition terminates TLS sessions that originate from mobile, broadband and IP supported POS, ATMs and smart phone based payment terminals.

Transaction protocols including VISA I, VISA II, ISO 8583, TPDU (Transport Protocol Data Unit), and Custom Protocols are utilized with hardware optimized efficiency. AccessGuard Cloud Edition integrates Security (TLS, IPSec etc) Transaction Protocol Processing (VISA, ISO8583, HTTPS (HTTP with TLS) transaction routing, etc) and IP Routing (RIP, OSPF etc).

An industry first and unique solution is consolidation of internet security, payment protocol handling and network routing for secure transaction routing within a single system.

Transport Layer Security (TLS)

TLS is a cryptographic protocol that provides secure communications over the internet. The protocol allows client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery. TLS involves a number of basic phases:

- Peer negotiation for algorithm support
- Public key encryption-based key exchange and certificate-based authentication
- Symmetric cipher-based traffic encryption

Encryption

The most widely used encryption algorithms for TLS are AES, 3DES.

01. Advanced Encryption Standard (AES): Advanced specification for the encryption that supports 192, or 256 bits.

02. Triple DES (3DES): Encrypts messages three times using DES 56-bit key, which is effectively 168-bit key encryption.

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 communi¬cations channel.

TLS Acceleration

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 CPU. Typically, this is a separate co-processor, specifically designed for handling encryption algorithms using parallel processing at very high speeds.

TLS Offloading

TLS offloading may look very similar to TLS acceleration. The term “offloading” is generally used to describe a completely separate computer that performs all TLS processing, so that the TLS load is taken off of the server completely. In a sense, an TLS hardware accelerator is performing TLS offloading, because part of the TLS processing is “offloaded” from the server’s CPU to the hardware accelerator.

An advantage of an offloader, as opposed to the typical accelerator, is that it can perform TLS processing for more than one transaction server, whereas the accelerator card is tied to a single server.

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 as well as the digital signature of an independent and trusted third party, called certification authority (CA), to ensure the validity of the transmitted information. The certificate format is based on ITU-T recommendation X.509. During TLS negotiation, certificates are exchanged for public key information. These certificates are validated with CA. Upon validation; this public key is used for shared key generation for symmetric encryption.

Mobile/Web Payment Processing

AcessGuard Cloud Edition offers a wide variety of service options for enabling multiple types of mobile payments, mCommerce and mobile wallet services.

The supported mobile payment interfaces includes;

- Mobile/web browser based payments
- Mobile application based transactions
- SMS/USSD based payments

AcessGuard Cloud Edition inter woks with these payment methods by interfaces to SMS/USSD gateways and HTTPS interface to the mobile device for the mobile browser or mobile application based transactions. These payment transactions from mobile devices are processed on the AcessGuard Cloud Edition and sent to the banking or financial institution servers for the payment approvals and authorizations.

AcessGuard Cloud Edition seamlessly enables the payment transactions for the two broad mobile payment service categories which are the retail merchant location based mobile POS based payment transaction and subscribers‟ mobile device initiated mobile wallet based payments.

HTTPS/Web/internet Transactions

AccessGuard CE enables the routing of HTTPS transactions (HTTP with TLS) which may encapsulate VISA/ ISO8583/ TPDU/Custom messages and transporting these protocol data to Host servers.

This integrated model allows the support of TCP/IP, TLS over TCP/IP and HTTPS transactions on a single AccessGuard CE instance.

STC – TransKrypt Cloud Edition

Security of transactions is a fundamental requirement for payment transaction industry and this becomes even more critical as the volume of payments are growing at a faster pace from the new generation mobile and broadband based IP payment terminals and devices. Securing the transaction session between terminals and the transaction processing systems is paramount as this data is traversing the least secure public networks.

Data encryption from POS/POI/Web/Mobile/mPOS terminals, Certificate verification of the client POI devices' Certificates, Tokenization of card holder data are multiple mechanisms for ensuring the security of the payment transaction data originating from the millions on payment initiating devices and flowing through the public networks comprising dial, broadband and mobile technologies across the world.

Several procedures are followed in the industry today towards achieving the security objectives and the establishment of the Point To Point Encryption(P2PE) standards by PCI Security Standards Council has helped to enable the industry to provide advanced security solutions for those devices dealing with card holder data. Point-to-Point Encryption (P2PE) solutions facilitate the objective of reducing the scope of PCI DSS assessment for merchants using such solutions by reducing the scope of their cardholder data environment and annual PCI DSS assessments. Based on standards requirements, P2PE solution are required to use secure cryptographic devices like host/hardware security modules (HSM) for the encryption and decryption of payment-card data, as well as for the storage and management of cryptographic keys.

Tokenization is another mechanism established to ensure that sensitive data can be replaced with surrogate data and avoid the compromise of the sensitive data. PCI's standards for Tokenization ensure uniform process for ensuring security with Tokenization.

TransKrypt Cloud Edition Security Functions

NewNet's TransKrypt Cloud Edition is a comprehensive security solution aimed at offering multiple security solutions which are auxiliary in function but crucial to payment transaction processing. The capability includes P2PE, Tokenization, and associated security and key management functions related to payment handling.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 Cloud Edition offers the following security functions:

- Point to Point Encryption (P2PE)
- Tokenization
- Key Management
- DUKPT
- PKI
- Authentication
- Application level encryption
- File security
- Digital signatures

P2PE (Point to Point Encryption)

In a generic scenario, the transaction request from client Web/POS terminal to payment processing gateway needs to be encrypted. TransKrypt CE follows all steps that form 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.

Key Generation

Key generation is based on DUKPT standards as specified by ANSI X9.24. Base keys are generated and stored in the TransKrypt CE 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 POI/POS devices towards generating the unique keys for each transaction.

Keys for Encryption at Client devices

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 CE

AG CE interfaces with the TransKrypt CE 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 CE, AG CE solution 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.

Cloud based Hardware Security Module (HSM)

STC TransKrypt CE uses FIPS HSM PCI-e card to generate & store keys secure.

Full Payload or Sensitive Field Encryption

TransKrypt CE'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.

Tokenization Functions

Tokenization application on TransKrypt CE utilizes a cutting edge FIPS 140-2 Level 3 Certified cloud based HSM for 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
- Secure Format Preserved Encryption(FPE) mechanism
- Advanced tokenization schemes using FF1 and FF3-1

SECURE TRANSACTION CLOUD