Connected Payments P2Pe Card Data Flow

The diagram on the following page depicts the current Connected Payments transaction flow when using P2Pe hardware encryption. Credit card capture is initiated at the POS devices located at shopper interface locations.

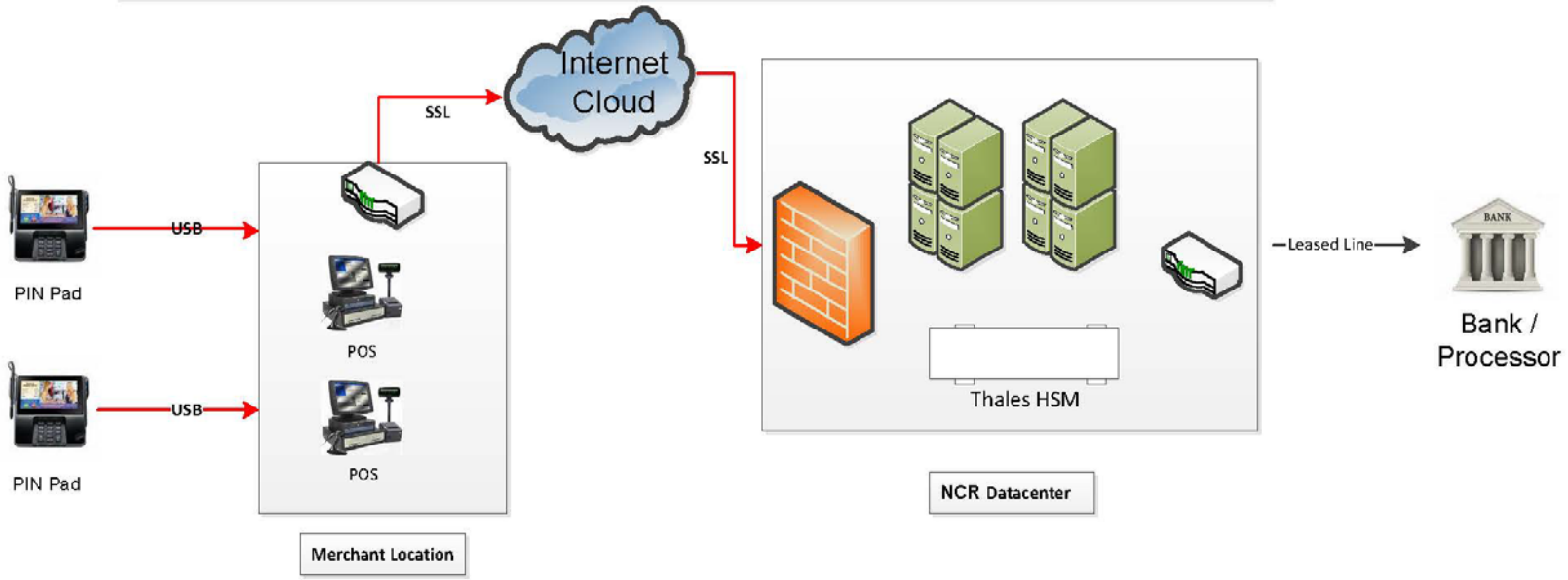
This card data flow assumes the use of Connected Payments, a PCI-compliant merchant solution. The diagram's components are defined below, and the combined use of these elements provide a secure processing environment for this card-present implementation.

Definition of Terms:

HSM	Shared Hardware Security Module (current model is Thales payShield 9000)
OpenEPS	Connected Payments component that operates on the POS terminal hardware
POS System	The Point of Sale system
DUKPT	Derived Unique Key Per Transaction
CHD Key	Triple-DES DUKPT key used to encrypt cardholder data
PIN Key	Triple-DES DUKPT key used to encrypt a cardholder PIN
3DES	Triple Data Encryption Standard algorithm that applies the cipher three times on each data block
PIN Pad	Device used to capture card data and shopper input
TRSM	Tamper Resistant Security Module located inside the PIN pad and where encryptions are performed

Author: Scott Meier
Director, Product Development
Retalix Global Payments

Connected Payments P2PE Card Data Flow



PIN Pad Device

- PIN Pad device is injected with a DUKPT key used only for Cardholder Data Encryption. This is not the same key used for PIN encryption.
- Upon swipe, the card data is 3DES DUKPT encrypted within the TRSM of the PIN pad device .
- PIN Pad device delivers to the POS lane the encrypted card data, KSN, First6, Last4, Exp Date, Service Code, Customer Name and Card Data Source.

POS Lane

- OpenEPS receives card slide response via USB connection.
- OpenEPS builds transaction message through a series of exchanges between POS and PIN Pad
- OpenEPS sends transaction message via SSL Web Service to NCR Datacenter

- Receives response from NCR Datacenter
- Builds receipt and passes transaction information to POS (BUT NO CARD DATA!)

NCR Datacenter

- Receives messages from OpenEPS
- Sends encrypted Card Data to HSM for decryption
- Sends transaction message together with decrypted Card Data to bank-owned router inside Datacenter, which communicates to Bank for processing via Bank's leased lines.
- PAN only is stored in NCR Datacenter, encrypted using AES128

- Receives response from Bank / Processor
- Stores transaction data in database (does NOT include any full Track Data)
- Returns response to OpenEPS (does NOT include any Card Data)

Bank / Processor

- Authorizes Transaction

- Returns response to NCR Datacenter