StoreNext

Update Bulletin

Getting Stores Out of PCI Scope Using Connected Payments Point-to-Point Hardware Encryption

March 14, 2012

Connected Payments now provides a new hardware-based Point-to-Point Encryption system for POS payments transactions. This breakthrough offers unsurpassed data and transmission security and for the first time almost entirely ***removes a retailer's stores and enterprise from PCI scope***. This is as close to the long-sought "silver bullet" for PCI as we are ever likely to see.

Using the PIN pad's internal hardware, Connected Payments can now encrypt PCI data using Derived Unique Key per Transaction (DUKPT) at the instant of card swipe, and this data stays encrypted through the PIN pad to handling at the POS terminal, and during transmission to the Connected Payments data centers – and back.

This "point-to-point" encryption via the PIN pad hardware provides the security of hardware encryption throughout the retailer's enterprise. A crucial benefit is that PCI has declared that this methodology takes everything between the point of encryption (the PIN pad) and the point of reception (the Connected Payments data center) ***out of scope for PCI.*** In fact, initial users of Connected Payments P-2-P hardware encryption have already been audited and confirmed these results from their PCI auditors.

How is this different from "software encryption," which we have used to secure transactions for several years? Software encryption uses Connected Payments algorithms running inside the PIN pad that —though also extremely secure — do not enjoy the benefits of PCI's out-of-scope declaration that applies currently only to ***hardware***-encrypted data. PCI's position at this time is that systems that protect transactions via DUKPT keys and are implemented by a PIN pad's native hardware — and with those keys managed by specifically approved methods — can currently enjoy "out-of-scope" status.

Retalix Global Payments submitted the Connected Payments P-2-P system for evaluation by *atsec*, a leading security systems lab and information security consultant. In their study, *atsec* examined the Connected Payments system in detail, including its implementation of encryption and key management in accordance with the PCI SSC and other technical industry standards, including the end-to-end card holder data flow, PIN pad white-listing (of cardholder data not subject to PCI DSS such as gift cards etc.) and DUKPT key management, including key transport management and methodology. The analysis was conducted under PCI DSS 2.0.

This *atsec* report is now available from the StoreNext website, and provides valuable detail about hardware encryption and why Connected Payments fully meets the PCI requirements for out-of-scope status. Quoting (spoiler alert!) one of *atsec's* most important findings:

> *In atsec's opinion, the Retalix Connected Payments Hardware Point-To-Point Encryption Solution achieves the goals necessary to allow a merchant to exclude any networks and applications, including POS and OpenEPS software and hardware connected to PinPads and involved in transmitting, storing, or processing transactions encrypted with the assessed solution from the responsibility of including them in PCI DSS compliance efforts, since cardholder data is not available in decrypted fashion, and keys are not obtainable in the merchant environment that would allow decryption of*

transaction data. data encrypted using the assessed solution cannot be decrypted outside of Retalix's Connected Payment data server, and exclusion from scope is justified.

The report also provides detailed instructions to QSAs for evaluating Connected Payments sites using Connected Payments Hardware P-2-P Encryption, including their findings for each of the twelve sections of the PCI DSS. Dealers should use this document to assist customers in streamlining and simplifying their PCI audits with the customer's QSAs.

HOW DO I GET MY CUSTOMERS' SYSTEMS OUT OF SCOPE?

- ***The Payment Solution*** — Connected Payments hardware encryption is available only to Connected Payments/ServerEPS subscribers. It cannot be implemented with WinEPS.
- ***PIN Pad Compatibility*** — Hardware encryption is available on Equinox/Hypercom terminals, with the L5300, L4150 and L4250 PIN pads now supported. There are no agreements for P-2-P protocol currently in place with other PIN pad manufacturers. The Connected Payments P-2-P keys are available via these methods:
  1. New Equinox/Hypercom PIN pads (L5300, L4150 or L4250) ordered from StoreNext can have the P-2-P hardware encryption key injected at no charge prior to initial shipment. Order the PIN (see the "Ordering" section below) to make this happen.
     - Once the hardware key is injected to a PIN pad, that PIN pad still remains compatible with standard (non-hardware encryption) implementations and configurations — including Connected Payments software encryption. The hardware P-2-P key will remain neutral and dormant until the Connected Payments host is updated to implement hardware P-2-P encryption for that location.
     - Again - injection of the hardware key does ***not*** make that PIN pad incompatible with anything, so best practice is to have the key injected in advance so that it's ready and waiting for the Connected Payments host to switch on hardware P-2-P encryption for that location.
     - Also, once the P-2-P key has been injected, it automatically kicks in when required by the host — no special parameters or settings must be changed on the PIN pad to enable a resident P-2-P key.
  2. Compatible Equinox/Hypercom PIN pads previously shipped and installed can have the Connected Payments P-2-P key added via the Equinox "Remote Key Injection" (RKI) system. There is a charge for each PIN pad when the key is injected via RKI, so it will be significantly less expensive to have the PIN pads injected at purchase whenever possible. See the StoreNext Update Bulletin discussing RKI for StoreNext dealers.
  3. The two methods described above — new purchases from StoreNext or RKI — are the only sources available or planned for provision of the hardware encryption key.
- ***Adding the Host Feature*** — The Connected Payments hardware encryption feature is provided at no charge for Summit users. Criterion users can add Connected Payments P-2-P Encryption for an additional $5/week.
  - Order the PINs below (on new Connected Payments Agreements or a Connected Payments Change Order) to initiate the new encryption being set up on the Connected Payments host.
  - ***Note!*** When the Connected Payments host is switched to enable hardware P-2-P encryption, the PIN pads must also have the hardware key injected in order for transactions to operate successfully. This is required for security, since if P-2-P could be deactivated via a PIN pad swap, it could not establish meaningful security. So make sure that the PIN pads are equipped with the P-2-P key prior to the host requiring P-2-P transaction processing.

ORDERING

For the Connected Payments P-2-P Hardware Encryption key, order this PIN when ordering the Equinox/Hypercom PIN pad at initial purchase from StoreNext:

PIN	Item	Price	Inst	Maint
HY-930220-115	Equinox Service, Key Injection, Connected Payments P-2-P Hardware Encryption	$ 25 Dealer Net: $ 0		

To enable Connected Payments P-2-P hardware encryption on the Connected Payments hosts, order the following PIN as appropriate. Note! Even though the PIN for Summit is no charge, it ***must*** be ordered to trigger the setup of hardware encryption for that site at the Connected Payments host.

PIN	Item	Price	Inst	Maint
SCP-P2P-S-01	StoreNext Connected Payments P-2-P Hardware Encryption Option for Summit (01)	N/C		
SCP-P2P-C-01	StoreNext Connected Payments P-2-P Hardware Encryption Option for Criterion (01)	$ 5		

To get the complete current Connected Payments Pricing sheet, just click here.