ACI UNIVERSAL PAYMENTS

DELIVERS PEACE OF MIND

PRODUCT FLYER

TAKING POS OUT OF PCI SCOPE

- **POS APPLICATIONS ACHIEVE SAVINGS BY KEEPING POS SOFTWARE OUT OF PCI SCOPE.**
- **CARDHOLDER DATA IS STORED SAFELY AND REDUCES EXPOSURE TO THEFT.**
- **THE NEED FOR POS SOFTWARE UPGRADES RELATED TO PA-DSS CHANGES IS ELIMINATED.**

With the development and enforcement of the Payment Card Industry (PCI) standards over the last two years, merchants and point-of-sale (POS) software vendors face significant investments in time and money to comply and, more importantly, to maintain compliance.

Any software, hardware or communication network that processes, stores or transmits sensitive cardholder data is “in scope” for PCI Data Security Standards (DSS) compliance.

A KEY ELEMENT TO THIS ARCHITECTURE IS NEW HARDWARE CALLED THE ISOLATED PAYMENT APPLIANCE.

FEATURES AT A GLANCE

ISOLATED PAYMENT APPLIANCE (IPA)

- LOGGING: LOGS APPLICATION, SYSTEM AND SECURITY EVENT ACTIVITY
- LOG SHIPPING: CONTINUOUS TRANSMISSION OF LOGGING EVENTS TO THE ISOLATED PAYMENT APPLIANCE MANAGER (IPAM)
- SOLID STATE ARCHITECTURE: NO MOVING PARTS FOR EXCELLENT DURABILITY AND A HIGH MEAN TIME BEFORE FAILURE
- FIREWALL: ISOLATES AND SECURES THE APPLIANCE FROM THE "OUT-OF-SCOPE" POS HARDWARE AND COMMUNICATIONS NETWORK
- AUTOMATED CHANGE MANAGEMENT: UPDATES ITSELF AUTOMATICALLY FROM THE IPAM
- SSL: SECURES CARDHOLDER DATA AND COMMUNICATIONS TO THE ACI PAYMENTS SWITCH, SSL-CAPABLE PINPADS AND IPAM SERVER
- ETHERNET PORTS: FOUR

IPAM

- CENTRALIZED CONFIGURATION AND CHANGE MANAGEMENT
- CENTRALIZED UPDATE MANAGEMENT
- AUTOMATIC CONSOLIDATION OF IPA LOGS
- INTEGRATION TO EXISTING CLIENT LOG MANAGEMENT SYSTEMS SUCH AS LOG LOGIC, GFI EVENTS
- MANAGER, TRIPWIRE, SPLUNK, ARCSIGHT AND OTHERS

Vendor software payment applications are mandated to be Payment Application Best Practice (PABP) or Payment Application-Data Security Standards (PA-DSS) validated. Merchants are required to be PCI DSS compliant. These burdens are extensive, real and ongoing.

- Annual Payment Application-Qualified Security Assessor (PA-QSA) costs for software vendors
- Annual QSA costs for merchants
- Quarterly network vulnerability scans
- Acquire and deploy new POS hardware and communications equipment
- Deploy operating system patches within 30 days of release
- Deploy vendor software upgrades within 30 days of release
- Install virus scanning software
- Deploy virus scan updates within 30 days of release
- Daily retrieval and review of intrusion detection and virus scan logs
- Secure the storage and custodianship of logs

Diagram 1 on page 3 illustrates a typical payments system architecture with POS hardware, host operating system, POS software and communication network components in scope for PCI. It is a fallacy that a retailer can avoid all PCI responsibility. However, it is possible to reduce PCI scope by taking various software and hardware components "out of scope". The purpose of this flyer is to present a deployment method of ACI's component solutions whereby the retailer can achieve substantive savings by keeping their POS software out of PCI scope, or further, to keep the POS hardware out of PCI scope as well.

TYPICAL PAYMENTS ARCHITECTURE TODAY

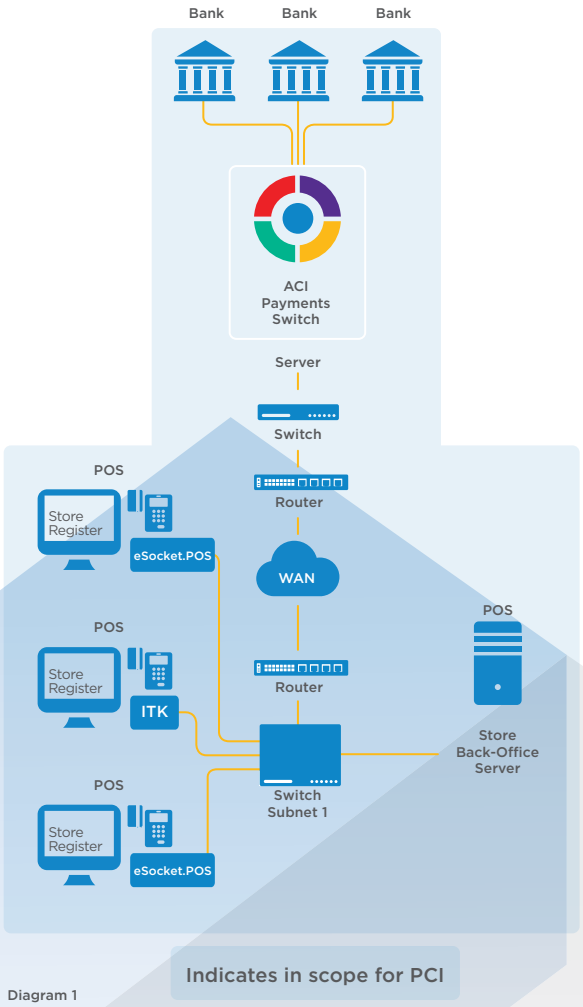

Diagram 1

COMPONENT PAYMENT SOLUTIONS

ACI Worldwide has been in the payments processing software business for more than 40 years. Its software is installed at hundreds of major merchants that process millions of transactions on a daily basis.

ACI's merchant retail software solution consists of several individual components. This software is assessed on an annual basis and is validated as PCI PA-DSS compliant. Each component has a unique purpose that allows flexibility in deploying each separately, in "layers" along the payments processing chain — from the POS, to the bank processor and back.

INTEGRATION TOOLKIT

ACI's integration toolkit (ITK) is an optional API that can be embedded into a retailer's POS application.

This API provides an easy way for a programmer to set various values needed within the transactional message and initiate an authorization request by invoking a set of objects. When these values are set, a function is called to kick off a transaction to eSocket.POS to fill in the remaining cardholder sensitive data values and send the message on for authorization.

eSocket.POS

ACI's eSocket.POS program talks to the PINpad using Ethernet connectivity. eSocket.POS is deployed at the store location and drives the PINpad through its various customer prompting screens that capture the chip data and card swipe, or prompts for a manual entry of the card credentials. The eSocket.POS application will then determine the card type, prompt for PIN entry if necessary and formulate a request for authorization from the payments switch. The automatic encryption built into eSocket.POS encrypts the sensitive data immediately after receiving this information from the PINpad. Thus, data passed between software components and across the network is made safe using an AES 256 bit encryption algorithm certified as PA-DSS compliant. The end-to-end encryption capability provides a further layer of security in the event that a network is compromised.

STORE AND FORWARD

Store and Forward (SAF) functionality is now embedded into the eSocket.POS application. The SAF functionality provides general "housekeeping" activities at the store location during transaction timeouts and offline periods. Timeout reversals and transactions that were locally approved can be stored and despoiled to the upstream payments engine when the communications network is restored. SAF also provides the ability to reroute payment transactions to alternate payment servers that are set up for "hot" or "warm" failover processing.

PAYMENTS PROCESSING

ACI's payments offering is the main authorization routing system deployed at the retailer's corporate office or at an offsite managed location. It accepts valid authorization requests from the store components. Transactions are routed to the merchant's various bank processors for approval and then stored for subsequent settlement and reconciliation. The payments engine can also be utilized by all of the merchant's business channels, including mail order, web, phone, mobile devices and other points of entry.

TOKENIZATION

The tokenization feature allows ACI to assign and return a token as part of every credit card authorization response returned by the payments engine. The token is stored in the card vault and provides a substitute value that is safe for storage by the POS.

TAKING POS OUT OF PCI SCOPE

STEP 1: POS SOFTWARE OUT OF PCI SCOPE

It is possible to build the interface between the POS and the ACI software components that allow the POS application software to be out of scope for PCI PA-DSS. In order to accomplish this, at no point may the POS application be exposed to sensitive cardholder data.

The POS begins the process with the ITK by setting data values that identify the transaction. These include values such as date, store, transaction, number and amount. When the POS is ready, an ITK function is called to kick off eSocket.POS and the data is passed along. eSocket.POS obtains the remaining sensitive cardholder information that is necessary to obtain an approval from the customer at the PINpad. Afterwards eSocket.POS receives the authorization response (including the token), the account number is masked and returned back to the POS for receipt printing. All transaction data, including the sensitive cardholder information, is stored back at the centralized payments engine for subsequent settlement, reconciliation and archival.

There are several benefits to both the POS software vendor and the retailer in taking the POS software out of PCI scope:

- POS application software is not subject to PA-DSS since it does not store, process or transmit cardholder data.
- POS application software is not subject to annual QSA assessment and the associated costs.
- The need for POS application software upgrades and rollouts related to PA-DSS changes is eliminated.
- Exposure to theft is reduced since sensitive cardholder data is no longer stored in each store's POS transaction log (TLOG). All data required for settlement is stored safely at the central payments engine.

Although there are several important security and financial benefits by keeping the POS application software out of PCI scope, the retailer cannot avoid PCI security mandates related to the hardware and host operating system that the POS software and the store back-office server run on. Although the POS software no longer handles sensitive cardholder data, if the ACI software components are deployed on either the POS register or a back-office server, then that hardware and host operating system are still considered "in scope" for PCI DSS controls, including system configuration management, patching, malware prevention, etc. Diagram 2 below illustrates a deployment scenario with the ACI components running on the back-office server, which makes that server "in scope".

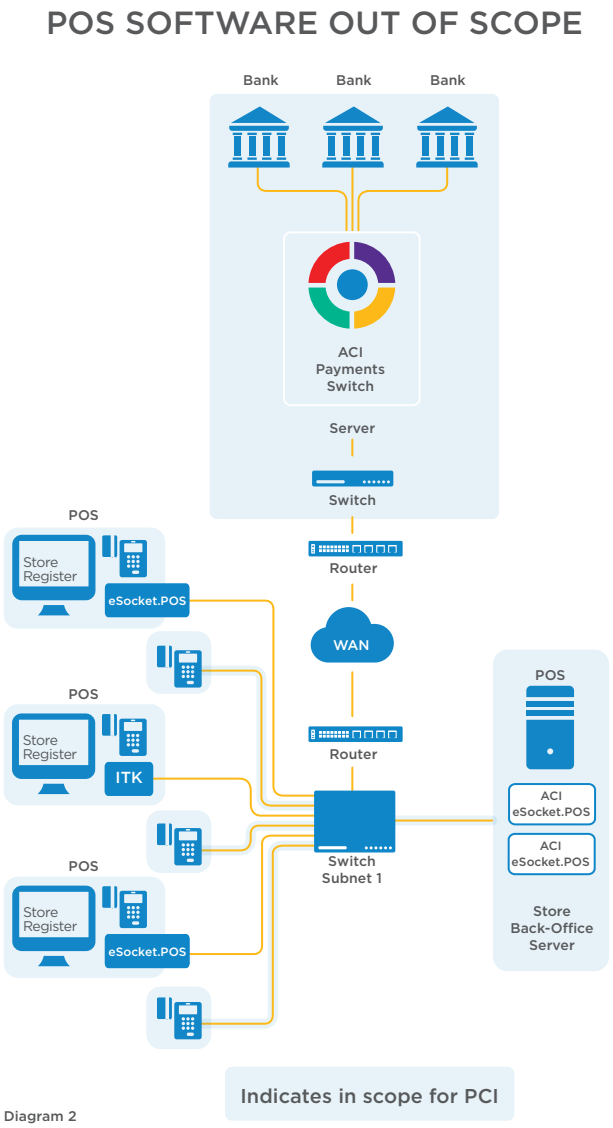

Diagram 2

POS HARDWARE OUT OF SCOPE

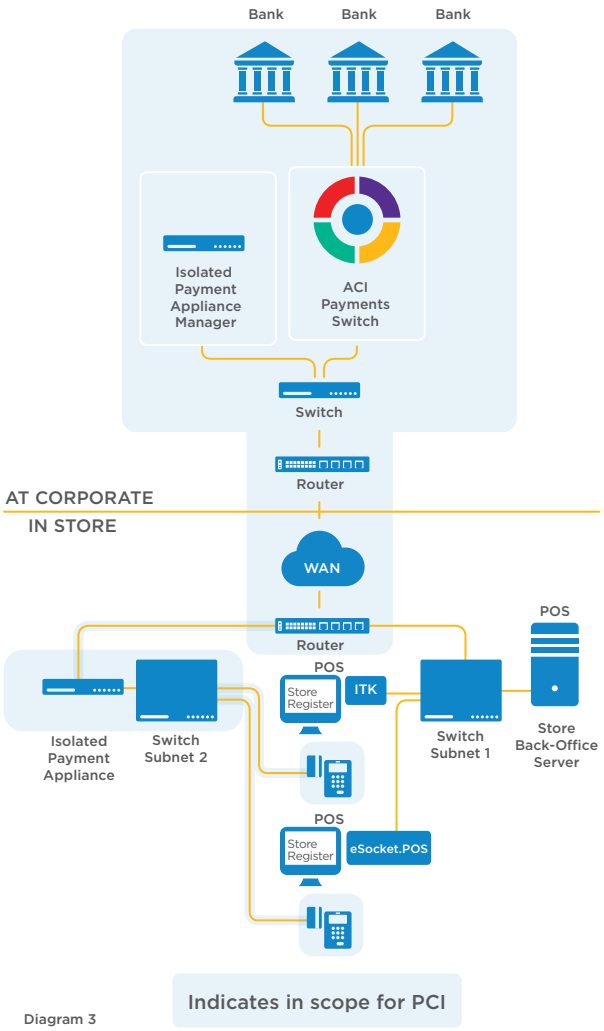

Diagram 3

However, there is a way to deploy the ACI components so that both the POS application software and the POS platforms can be considered out of scope for PCI compliance.

STEP 2: POS HARDWARE OUT OF PCI SCOPE

Step 2 builds on the integration method described in Step 1. Diagram 3 above describes a method to deploy the component software that allows the merchant to keep the POS platforms out of scope for PCI compliance.

A key element to this architecture is new hardware called the IPA. This simple device hosts the in-store ACI software components, provides firewall partitioning and establishes a secure SSL "tunnel" through the network to route payments authorization data to the ACI payments engine.

Diagram 3 shows the segmentation of a new subnet 2, to separate non-SSL capable Ethernet PINpads from the store POS network. The blue shaded items indicate the remaining elements in the store that store, process or transmit sensitive cardholder data. These remain separated from the POS application running on the terminals/lane PCs, and the back-office server resides separately on the existing out-of-scope subnet (subnet 1).

The in-store IPAs are managed from the corporate office by a new IPAM. This centralized manager provides automated procedures such as log consolidation and archival, downloading application and system updates, and log integration to industry standard log-management applications. Together, the IPAs and IPAM solution help provide a turn-key approach for easy device management while isolating payments from the POS hardware to enable keeping them out of scope for PCI.

In addition to the benefits described in Step 1, there are several benefits to the retailer in Step 2 and taking the POS hardware out of scope:

- Continue to use existing, non-PCI compliant OS platforms and software
- Eliminate the requirement to update and distribute operating system updates and security configuration controls to each POS register
- Eliminate the requirement to maintain and distribute operating system updates and security configuration controls to each POS back-office server
- Eliminate the requirement for host security controls, virus scanning and intrusion detection software on POS registers and servers

SUMMARY

Removing the flow of sensitive cardholder data from the POS software, host operating systems and the hardware it runs on can significantly reduce compliance validation requirements and result in PCI compliance cost savings. The Step 1 and Step 2 deployment architectures described in this flyer can allow a reduction in the manpower needed to manage integrated store payment architectures and secure the sensitive cardholder data.

REVOLUTIONIZES PAYMENTS

ACI Worldwide, the Universal Payments company, powers electronic payments and banking for more than 5,000 financial institutions, retailers, billers and processors around the world. ACI software processes $13 trillion in payments and securities transactions for more than 250 of the leading global retailers, and 21 of the world's 25 largest banks. Universal Payments — — is ACI's strategy to deliver the industry's broadest, most unified end-to-end enterprise payment solutions. Through our comprehensive suite of software products and hosted services, we deliver solutions for payments processing; card and merchant management; online banking; mobile, branch and voice banking; fraud detection; trade finance; and electronic bill presentment and payment. To learn more about ACI, please visit www.aciworldwide.com. You can also find us on Twitter @ACI_Worldwide.

www.aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

AFL5821 10-15