

ACK - PCIDSS Solution Overview

ACK, as a company, has always focused on getting the core fundamentals right and keeping things simple; as a consequence, our products meet retailers' requirements for simple-to-operate and reliable code. Helping our customers meet the requirements of PCIDSS is no exception to these principles.

The focus of PCIDSS is to ensure that wherever credit/debit card data is stored it is secure and not readily accessible to the criminal fraternity. The fact that card holder data is stored both in retail store and at retailers' head offices is challenging, but the ACK solution is designed to secure this sensitive data at each location individually and collectively.

The following details are designed to give a broad outline of how ACK products help retailers meet the requirements of PCIDSS with integrated EFT in a retail environment.

Background

Card holder data accumulated by an integrated EFT system within a retail store environment until the end of the trading day is referred to as the transaction log file. At the completion of the trading day, these log files must be submitted to the acquiring bank so that the retailer gets paid. The two most common methods of submission of the log files are; polled or central. Polled submission is where a bank-approved polling bureau retrieves the log file from each store using the APACS 50 protocol. Central submission is where the log file from each store is pulled or pushed to the retailer's head office where they are consolidated into one file for submission in bulk under the retailer's control directly to the acquiring bank for settlement.

Daily transaction log files at most retail stores will rarely contain enough card data, even in a busy store, to rise above Level 4 in the PCIDSS risk assessment. But the cumulative total of card transaction data collected from across an entire estate and held centrally will be significant and could raise the PCIDSS risk to Level 1.

The ACK PCIDSS compliant software solution is the result of detailed research into the provision of effective data security which can be implemented with full consideration of the operational constraints of a retail environment both at the retail store level and at the head-office level.

Design Objectives

ACK set itself a number of product design objectives when considering the implementations of encrypting transaction log files. The design objectives:

Do Not:

1. Require existing ACK chip and PIN solutions to be re-accredited.
2. Adversely affect system performance

Contact **ACK Ltd** for further details on:

Tel: 0118 948 2588, e-mail: enquiries@ackltd.co.uk web site www.ackltd.co.uk.

Confidential Information

3. Mandate the use of additional third party products (hardware or software) and associated licence fees
4. Alter the operator or cardholder experience

Do:

1. Provide a simple method of securing sensitive information
2. Allow hardware security modules to be used if required
3. Keep the management of encryption keys as simple as possible (and therefore used!)
4. Provide fully automated functions wherever possible

These objectives also happen to satisfy the business objectives of most retail organisations.

Philosophy

Human nature being what it is, any system which is not automated and/or easy to use is liable to be neglected, ignored completely or subverted.

Furthermore, the impact of security on the functionality of a system and the organisation must be considered. ACK have analysed the options and devised a system that takes into account the operational and business needs of a retailer: We felt it important that the shop staff and IT department should not be burdened with unnecessary additional procedures nor have their jobs made more complicated.

With the above in mind, ACK have devised a data security system which:

1. Uses techniques which ensures data is secured at each stage.
2. Operates seamlessly as far as shop staff are concerned.
3. Has minimal impact on system implementation and maintenance.
4. Places only minimal responsibility on those responsible for IT functions.

ACK have applied the following two rules for maintaining effective security:

1. Key storage must be secure itself - like any other security system, the locks may be adequate to resist unauthorised intrusion, but will be useless if the key is not held securely.
2. Key management must be simple to operate - complex systems are more vulnerable to abuse.

Having devised an effective security system, ironically, the weakest point for card security are the APACS Standards which currently expect unencrypted card data to be presented and processed by APACS compliant host systems.

Acquiring banks are therefore in the invidious position of insisting that the retailers adhere fully with PCIDSS requirements, whilst at the same time expecting transaction data to be made available to them in an insecure format.

Contact ACK Ltd for further details on:

Tel: 0118 948 2588, e-mail: enquiries@ackltd.co.uk web site www.ackltd.co.uk.

Confidential Information

Method of operation

Single Site Installations

For retail environments that do not involve centralised submission the ACK software is self managing.

The only prerequisite is that the ACK software is running under Windows NT and above - this is because the ACK software uses the CryptoAPI which comes as standard within these Windows operating systems.

Thereafter, the PCIDSS compliant ACK software will self-manage the encryption of transaction data as it is written to the transaction log. Key-mutation is automatic and ensures the data will be impossible to be decrypted on any other machine and may therefore be transmitted safely across private and public networks.

The ACK software will also perform automatic deletion of transactions over seven days old, thereby ensuring the cumulative number of card transactions potentially do not exceed PCIDSS Level 4 data volumes.

The only area of risk is that encrypted transaction data cannot be decrypted should the public and private keys become lost or destroyed as these keys are specific to each machine where encryption takes place. Therefore, any catastrophic failure of the individual machine will render the transaction log files unreadable. However, the keys can be stored separately and re-instated on a new machine in the event that a new machine is to be deployed - clearly the management of these keys must be secure. Note that all is not lost should catastrophe strike as individual transactions can be recovered from the hardcopy merchant receipts.

Multi-Site Installations

For retail environments which operate across multiple sites and where centralised submission is in operation using the ACK Bulk Delivery System, the following will take place:

The ACK software components at the store remain the same as for single-site installation, but an estate public key will be used. The estate public key is created on, and used by, the ACK Bulk Delivery System machine using the ACK Estate Key Manager which creates two keys: 1) the private key which BDS uses to decrypt the incoming transaction log files and 2) the estate public key which must be distributed to each store where ACK software is running.

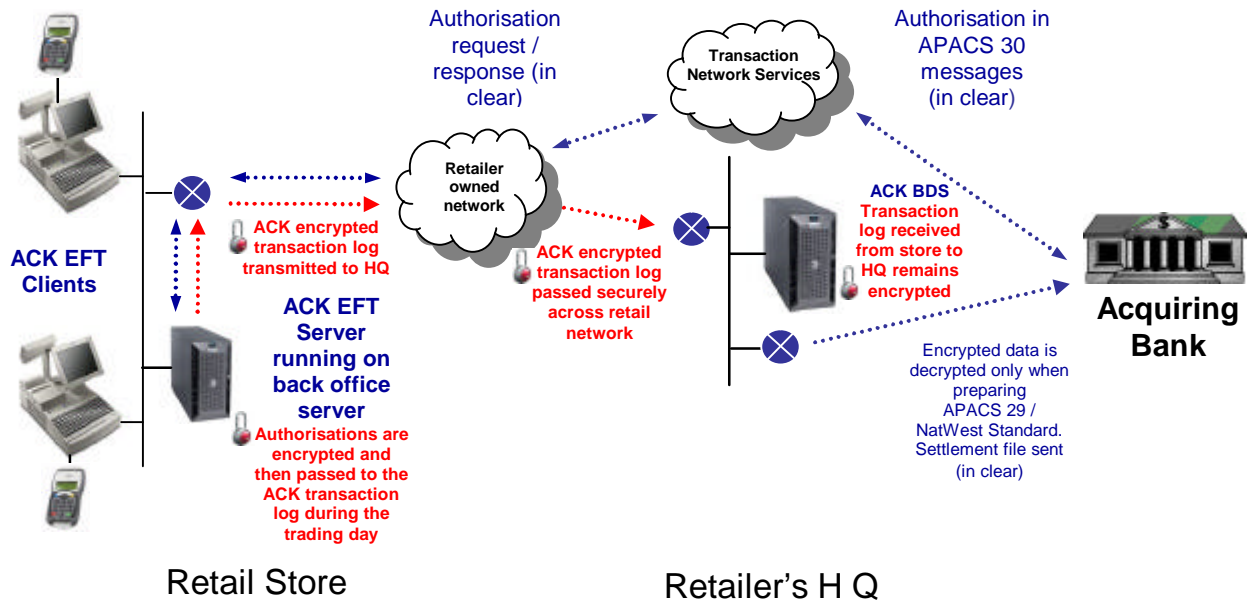
At the end-of-day, the ACK software at the store will decrypt the transaction data using its local public key (as used in the single-site installation), and re-encrypt the data with the BDS estate public key. The transaction data is therefore still secure and can be transmitted over the network (public or private) to the central site where it will be imported, still encrypted, into the database. BDS only decrypts the data once it is ready to create and transmit the settlement file to the acquirer.

Contact **ACK Ltd** for further details on:

Tel: 0118 948 2588, e-mail: enquiries@ackltd.co.uk web site www.ackltd.co.uk.

Confidential Information

Card Authorisation and Submission Network Diagram showing Encrypted Data path



If you are concerned about how to comply with PCIDSS requirements, ACK are here to help and inform you. We have put together useful background information which can be found on the other pages on the ACK web site.