

3C Integra Payment Solution

for your PCI DSS Requirements



SIX Card Solutions payment application's solution 3C Integra is supported by PA DSS and PCI DSS certifications and can be used by merchants within their own PCI DSS projects, dramatically reducing the scope of their environment and the risks presented by the scope of the environment.

3C Integra is a PA DSS payment application for processing of Card Present transactions. A Java based application running on a hardened SuSE Linux Operating System, which operates as a transaction aggregation point accepting transaction data from a variety of POS and PMS systems. Authorisation are performed in real-time over a SSH secured channel, while the settlement takes place overnight over a HTTPS secured link.

The management and maintenance is fully managed by SIX Card Solutions and as a result the merchant has no logical access to the 3C Integra Operating System or application.

3C Integra communicates directly with SIX Card Solutions host within their PCI DSS compliant envi-

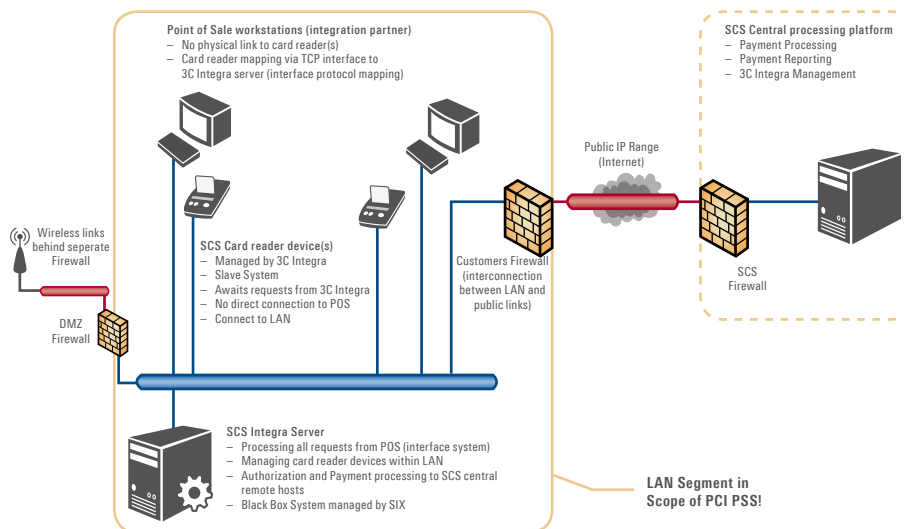
ronment. There are many additional functions, mainly in security area, such as host intrusion detection system, collation of logs and even monitoring of those when they are sent back to SIX Card Solutions.

There is no GUI for the clients; it is rather seen as 'black box' type of product as SIX Card Solutions performs all configuration and maintenance tasks.

Cardholder data is encrypted within the database using AES 256-bit algorithm.

Hardening includes but is not limited to: disabling root access for ssh remote login, disabling reboot via keyboard, enabling logging of spoofed packets (kernel + firewall), removing any ISDN or PSTN dial up support possibility. SIX Card Solutions configure native Linux IP tables firewall rules to prevent an impact on possible misconfiguration of client's firewall.

In addition, SSH deny host attack protection is configured. OSSEC agent is installed on every server and acts as the main tool to collect logs and send them to SIX Card Solutions, including 'denyhosts' alerts.



SIX Card Solutions uses network firewall-based network segmentation to isolate the cardholder environment from other non-PCI related network infrastructure.

3C Integra comes with its operating manual and instructions providing guidance to allow the software to be installed to support the overall compliance status of the merchant.

We recommend the installation of perimeter firewalls between any wireless networks and the cardholder data environment, and to configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

By prohibiting storage of sensitive authentication data post-authorisation, the assumption is that the transaction has completed the authorisation process and the customer has received the final transaction approval and this sensitive authentication data is never stored. The requirements for the encryption of stored cardholder data and the restrictions applied to the storage of sensitive authentication data have been addressed through the use of our transaction processing service which is composed of a PA DSS validated payment application (3C Integra) transmitting data to central authorisation and settlement environment which is PCI DSS compliant.

There are no screens within 3C Integra displaying cardholder data. PAN is masked to show only the last 4 digits, also can be configured to show the first 6 and the last 4 digits. Due to structure of the database any other systems can get truncated PAN without decrypting it as there are separate fields for just the first 6 digits and the last 4 digits.

PAN data is encrypted on the database level by AES 256-bit algorithm.

3C Integra facilitates sending of cardholder data over the Internet encrypted with SSL or via SSH. There is no backward compatibility with SSLv2 and lower. Only SSHv2 and SSLv3 protocols are used.

Internally developed tracking system insures that timely development and deployment of security patches and software upgrades to customers, delivery of patches and upgrades in a secure manner with a known chain-of-trust and in such a manner that maintains the integrity of deliverable, integrity testing of patch/update prior to installation are included into process.

SIX Card Solutions periodically provide customers with patches and upgrades. Patches and upgrades are always delivered and implemented by SIX Card Solutions staff. Integrity of patches/updates is maintained through a strict process of delivery and SHA 256-bit checksum being verified by the target system prior to installation.

Access control systems have been configured to enforce privileges assigned to individuals based upon the individual's job classification and function, all using unique user Ids.

Audit trails are enabled by an Open Source Host-based Intrusion Detection System (OSSEC) agent on 3C Integra server to collect syslog data. OSSEC is configured so that it captures all actions taken with administrative privileges, access to audit trails, invalid logical access attempts, use of identification and authentication mechanisms, initialisation of audit logs and creation/deletion of system level objects.

Are you interested in 3C Integra - The hospitality solution? Then please do not hesitate to contact us. Our sales representatives will gladly provide you with further information in a non-binding, personal consultation.