

# Managed Payment Services

## White Paper



### The Changing Architecture of Integrated Card Payment Solutions

April 2010

## Introduction

PCI DSS is a catalyst to re-architect card payment solutions.

Current Chip and PIN solutions are an evolution of the original magnetic stripe based solutions where the application was historically installed on the POS.

Many card payment solution vendors are responding to PCI DSS by adding further levels of complexity to the architecture of their existing solutions that involve putting some or all of the application processing on the PED.

The advent of fast, reliable and resilient secure private managed networks provides the opportunity to re-architect card payment solutions to take advantage of thin client architecture. This architecture was not feasible when many of the existing card payment solutions were designed because the networks in general use at the time did not offer the required speed, reliability and resilience.

A thin client card payment solution allows cardholder data to be moved quickly from the PED to a secure location for payment processing.

The purpose of this white paper is to look at the different architectures for delivering a card payment solution and how they meet the requirements of PCI DSS to secure cardholder data. These architectures are also examined for their ability to provide a solution that is flexible enough to accommodate the future changes in the retailer's requirements for payment acceptance and the evolving requirements of the PCI security standards. The paper uses these options to explain why Vodat chose to deliver its Managed Payment Service using a secure data centre to host a thin client payment solution with PEDs connected over IP.

## Scope of this Paper

This paper considers the architecture of card present payment solutions that are coupled to the POS. That is where the payment transaction is initiated by the appropriate tender type on the POS application and passed to the payment solution for processing.

## Architecture Options for Delivering a Card Payment Solution

In order to satisfy the PCI security standards it is clear that the best location to process and store sensitive cardholder data is at a secure data centre. The issue for PCI security standards is how the card present payment transactions are processed, stored and transmitted from the time the card is read by the PIN entry device or the magnetic stripe is swiped, to the completed transaction reaching the secure data centre.

This paper will use the terms **EFT Client** and **EFT Server** to describe the two main components of a card payment solution.

**EFT Client** is the application that manages the messages between the PIN entry device (PED) and the EFT Server.

**EFT Server** is used to describe the payment engine / switch installed at the secure data centre to manage authorisations, submit settlement files and provide transaction enquiries and reporting.

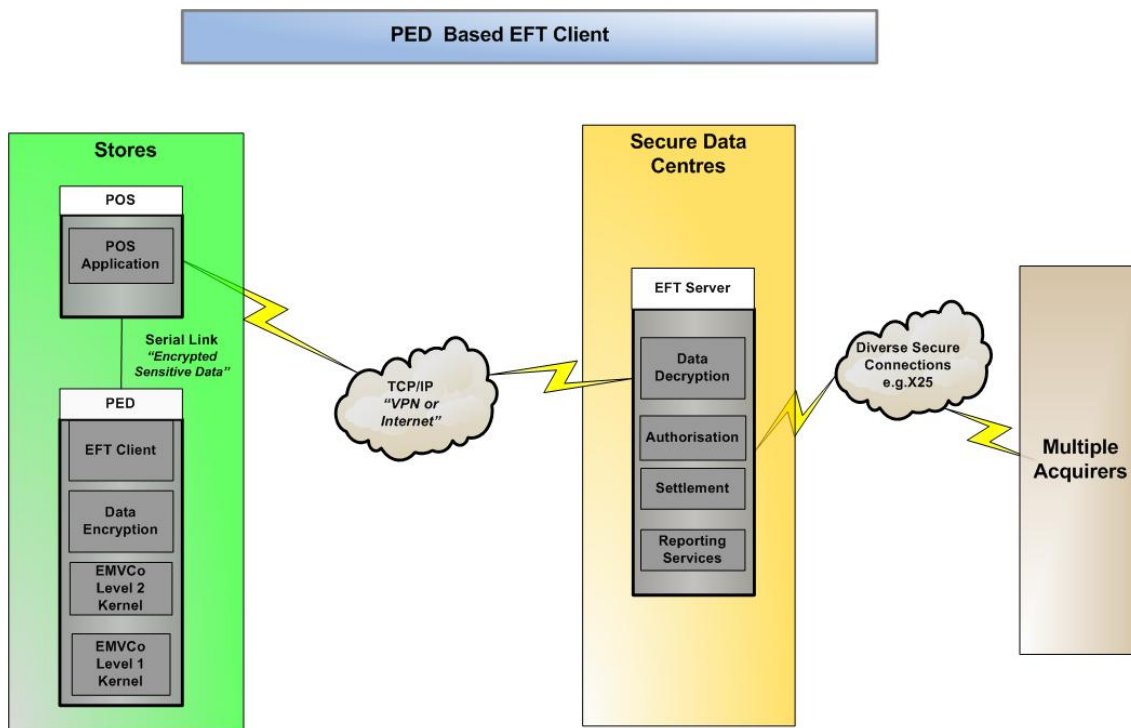
The paper considers the advantages and disadvantages of five architectures for the deployment of the EFT Client and its associated applications to deliver a card payment solution that reduces the extent of the retailer's systems that are in the PCI DSS scope.

The five options for the EFT Client are:

1. PED based
2. POS based with sensitive data encrypted on the PED
3. POS based with sensitive data encrypted on the POS hardware
4. Secure local server based with PEDs connected securely over IP
5. Secure data centre based with PEDs connected securely over IP.

### Option 1: PED Based EFT Client

In this option the PED is attached to the POS hardware through a local connection. The EFT Client and EMVCo Level 2 Kernel are installed on the PED. All local processing of the payment transaction is done on the secure PED and the sensitive card data is encrypted on the PED before it is passed via the POS to the EFT Server.



The advantages of this architecture are:

- The POS application and POS hardware are out of PCI DSS scope; apart from PED, everything at the store is out of scope
- The solution is able to accept card payments when the POS is offline, having lost its connection to the EFT Server at the secure data centre, storing transactions on the PED until the connection to the EFT Server is re-established
- The sensitive cardholder data is encrypted on the PED before being passed via the POS to the EFT Server at the secure data centre
- The payment software on the PED may not need to be upgraded when the POS solution is replaced.

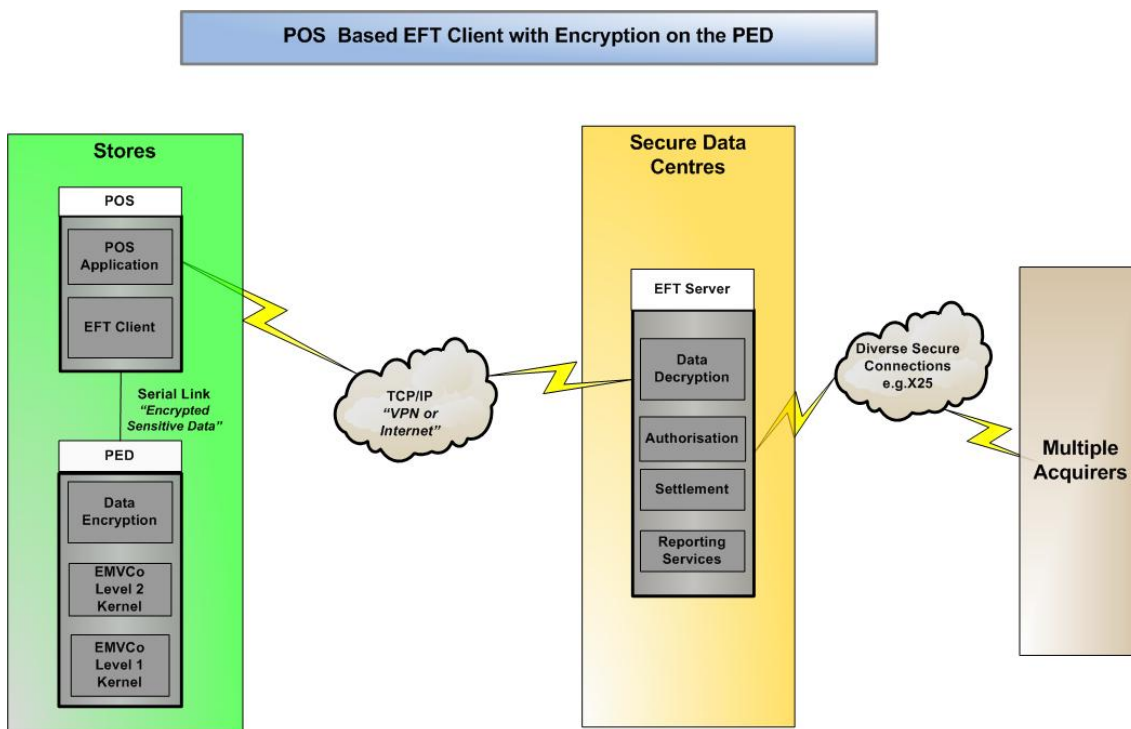
The disadvantages are:

- Such EFT Clients cannot easily be ported to PEDs from different manufacturers because the software development environments are proprietary to each manufacturer. The retailer will probably be locked into one PED manufacturer
- Changes to functionality will be reliant on a third party with specialist technical skills which can be costly if firmware changes are required and may require hardware upgrades to the PED

- Harder to support any value added services (e.g. loyalty, customer questionnaires, etc.) through the PIN pad, as any change will require the application to be developed in the proprietary operating system of the PIN pad and may require the involvement of the PED supplier
- Relatively frequent updates to functionality may be required as schemes and acquirers adopt new business rules
- Updates to PED configuration and firmware will be challenging as retailers are not used to managing changes outside of the POS hardware and may need to be applied by a third party
- May not be able to support other card acceptance devices, such as outdoor payment terminals, kiosks and mobile POS requiring different EFT Client applications for each environment
- Harder to investigate errors as the solution is a 'black box' which may offer less access to logging and debugging tools than a thin client solution
- Requires a more powerful processor and more memory in the PED to handle all of the payment transaction processing and, as a consequence, will cost more to purchase
- Although encrypted, sensitive cardholder data is still being passed through the POS to the EFT Server at the secure data centre.

### Option 2: POS Based EFT Client with Encryption on the PED

In this option the PED is attached to the POS hardware through a local connection. The EMVCo Level 2 Kernel is installed on the PED but the EFT Client is installed on the POS hardware. Sensitive card data is encrypted on the PED before it is passed to the POS. The EFT Client processes the payment transaction on the POS hardware and passes the encrypted sensitive data to the EFT Server where it is decrypted before it is passed to the acquiring banks.



The advantages of this architecture are:

- The POS application and POS hardware are out of PCI DSS scope; apart from PED, everything at the store is out of scope
- The sensitive cardholder data is encrypted on the PED before being passed via the POS to the EFT Server at the secure data centre
- The solution is able to accept card payments when the POS is offline; having lost its connection to the EFT Server at the secure data centre
- Easier to configure and maintain the payment application than it is with PED based payment solutions.

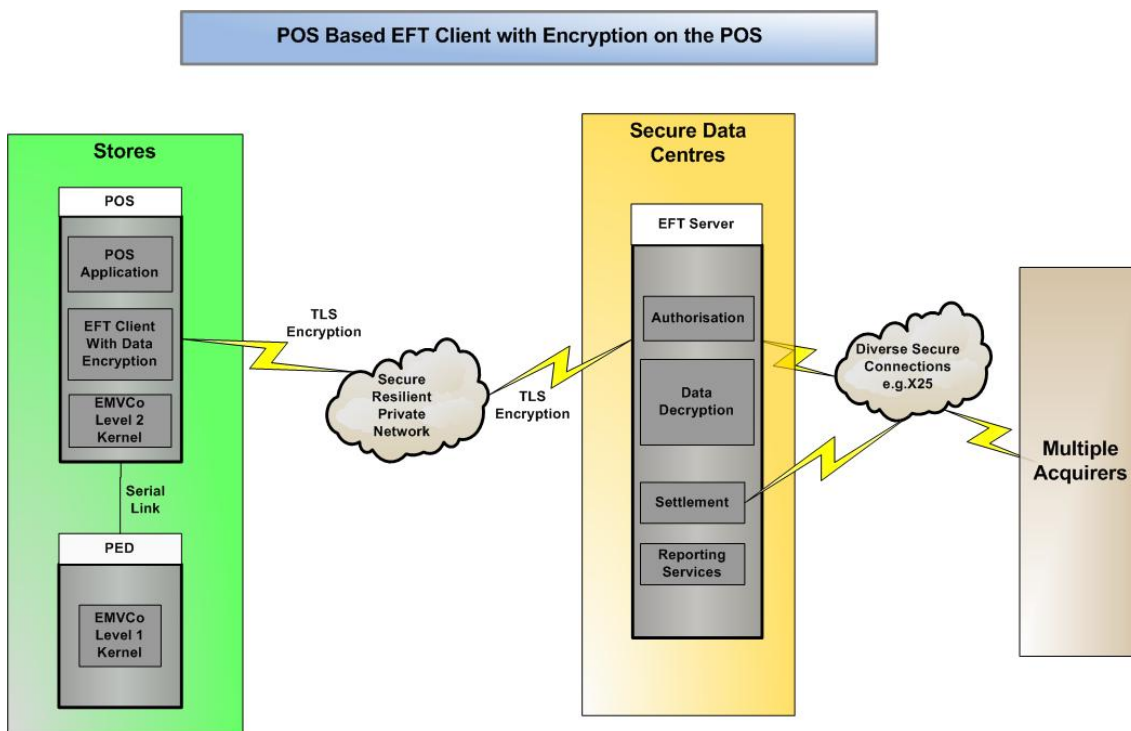
The disadvantages are:

- With business logic, including the EMVCo Level 2 Kernel, on the PED, will require configuration changes and updates to be applied to the PED as card schemes introduce new rules
- May require changes to the EFT Client when changing PED and the API for the EMVCo Level 2 Kernel may differ between PED manufacturers and different PED models from the same manufacturer

- May require changes to the encryption software on the PED when porting to devices from different manufacturers because the PED environments are proprietary to each manufacturer
- The EFT Client on the POS will need to be reinstalled when the POS is replaced
- Although encrypted, sensitive cardholder data is still being passed through the POS solution to central payment server.

### Option 3: POS Based EFT Client with Encryption on the POS Hardware

In this option the PED is attached to the POS hardware through a local connection. The EFT Client and the EMVCo Level 2 Kernel are installed on the POS hardware. The EFT Client processes the payment transaction on the POS hardware and encrypts the sensitive card data before passing it over a secure tunnel using TLS encryption to the EFT Server. The EFT Server stores the encrypted card data with the completed transaction and only decrypts it when preparing the settlement files to be passed to the acquiring banks.



A further refinement to this option is, where supported by the installed PEDs, to encrypt the sensitive card data passing between the PED and the POS. This will depend on the encryption solutions provided by the PED manufacturers, the PED connection options (e.g. RS 232, USB slave or Ethernet) that support these encryption solutions and how at each retailer the PEDs are connected to POS.

The advantages of this architecture are:

- The POS application itself is out of PCI DSS scope since no sensitive data is exchanged between the POS application and the EFT Client
- The solution is able to accept card payments when the POS is offline; having lost its connection to the EFT Server at the secure data centre. Encrypted transaction data is stored securely until the connection is re-established and can be trickle fed to the EFT server
- Software EMVCo level 2 kernels tend to support a wide range of available PED devices offering flexibility and choice to the retailer
- Much easier to configure and maintain the payment application than it is with PED based payment solutions. Merchants are used to updating software on a PC based POS solution (e.g. via FTP) whereas they are not used to updating firmware on a PED
- Offers a transition path for retailers who ultimately want to take their POS hardware out of PCI scope but who do not wish to replace their existing PEDs immediately

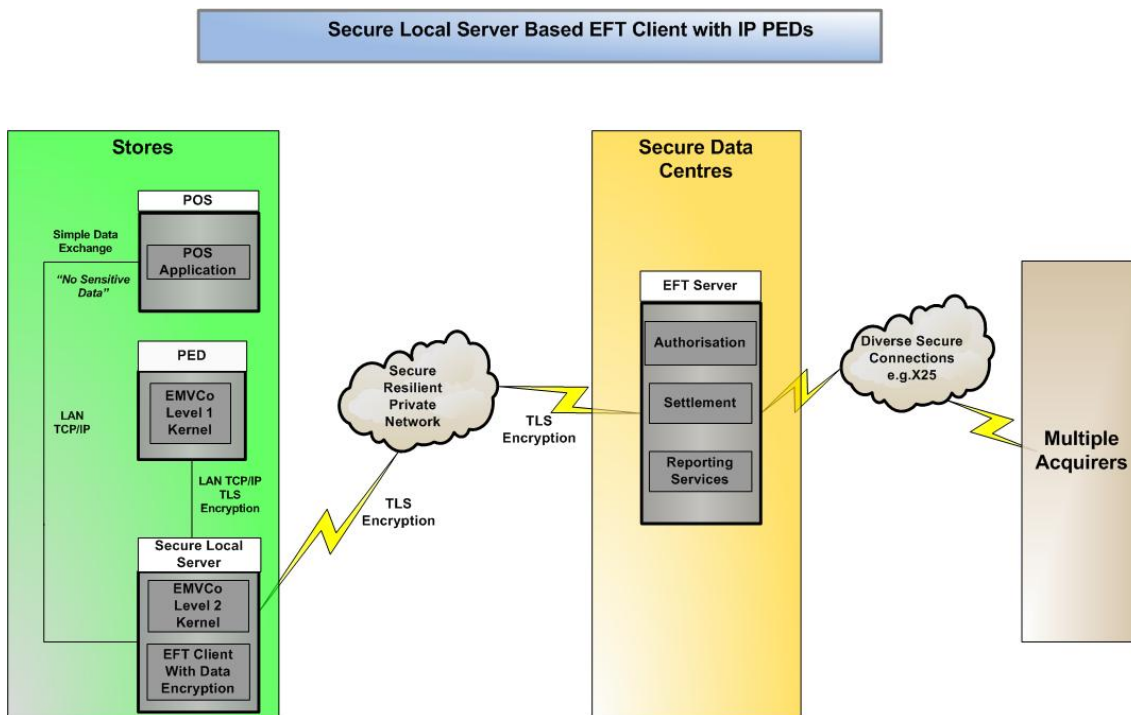
- Provides a flexible option for retailers who accept that their POS hardware remains in PCI scope.

The disadvantages are:

- The POS hardware is still in PCI DSS scope because the EFT Client is processing sensitive card data and is still in PCI scope. It therefore has to meet the PCI requirements including virus checker, password protected local access and two factor protected remote access
- The payment software on the POS will need to be reinstalled when the POS is replaced
- Although encrypted, sensitive cardholder data is still being passed through the POS solution to central payment server
- If the local link to the PED is encrypted there may need to be changes to the firmware on an existing PED device or even a replacement PED which supports link level encryption.

#### Option 4: Secure Local Server Based EFT Client with IP PEDs

In this option the PEDs are connected via IP over a local area network to a secure local server dedicated to managing payment transactions. The EFT Client software and the EMVCo Level 2 Kernel are installed on the secure local server. The payment transaction data is passed over a secure tunnel using TLS encryption from the PED to the secure local server where the sensitive card data is encrypted before being passed again through a secure tunnel to the EFT Server at the secure data centre. The EFT Server stores the encrypted card data with the completed transaction and only decrypts it when preparing the settlement files to be passed to the acquiring banks.



The advantages of this architecture are:

- The POS application and POS hardware are out of PCI DSS scope; apart from PED and secure local server, everything at the store is out of PCI DSS scope
- No sensitive cardholder data, even if encrypted, is passed to or through the POS solution
- The secure private managed network is segmented to separate completely cardholder data from other business systems
- Requires only the device manufacturer supplied EMVCo certified Level 1 firmware, IP communication software and TLS encryption software to be installed on the PED
- Offline transactions can be stored safely on the secure local servers until the connection to the EFT Server at the secure data centre is re-established
- Transaction times will not be significantly affected by the processing power of the PED
- Easier to configure and maintain because any changes to the solution can be applied remotely to the secure local servers
- Easier to add new functionality such as additional payment types and new acquirers

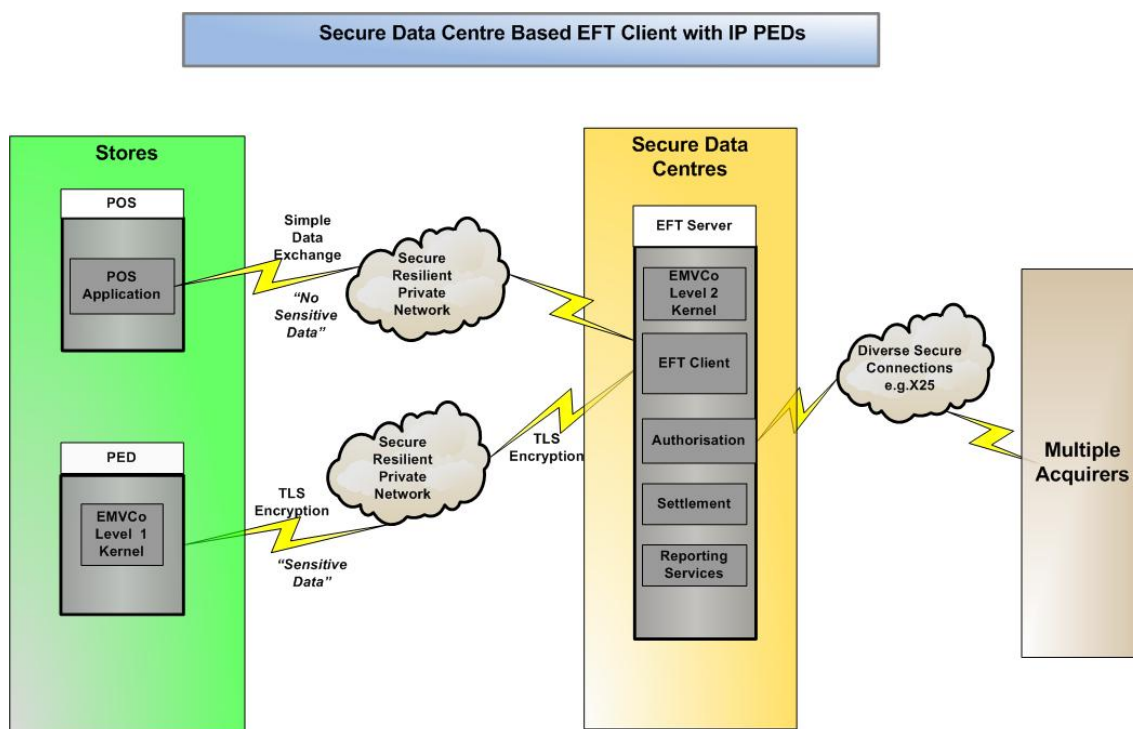
- Easily support PEDs from many device manufacturers
- Can be coupled quickly to a new POS solution when the existing solution is replaced or to other card acceptance devices, such as outdoor payment terminals, kiosks and mobile POS
- Easy to integrate with existing business systems.

The disadvantages are:

- Requires secure local servers for the EFT Client to which access must be managed and controlled including anti virus protection, two factor authentication for remote administrator access, restricted access for local administration and network segmentation
- Does not support offline transactions when there is no local area network connection from the PEDs to the EFT Client on the secure local server but this can be mitigated through a resilient LAN architecture, such as using multiple LANs to support different points of service across a store.

### Option 5: Secure Data Centres Based EFT Client with IP PEDs

In this option the PEDs are connected via IP over a secure private managed network to a secure data centre. The EFT Client software and the EMVCo Level 2 Kernel are installed on servers at the secure data centre. The payment transaction data is passed over a secure tunnel using TLS encryption from the PED to the EFT Client at the secure data centre. The EFT Client passes the payment transaction data to the EFT Server which encrypts the sensitive card data before storing the completed transaction. The EFT Server decrypts the sensitive card data when preparing the settlement files to be passed to the acquiring banks.



The advantages of this architecture are:

- The POS application and POS hardware are out of PCI DSS scope; apart from PED, everything at the store is out of PCI DSS scope
- No sensitive cardholder data, even if encrypted, is passed to or through the POS solution
- The secure private managed network is segmented to separate completely cardholder data from other business systems
- Requires only the device manufacturer supplied EMVCo certified Level 1 firmware, IP communication software and TLS encryption software to be installed on the PED
- Easiest to configure and maintain because any changes to the solution need only be applied at the secure data centre
- Easiest to add new functionality such as additional payment types and new acquirers
- Easily support PEDs from many device manufacturers
- Can be coupled quickly to a new POS solution when the existing solution is replaced or to other card acceptance devices, such as outdoor payment terminals, kiosks and mobile POS

- Easy to integrate with existing business systems.

The disadvantages are:

- Does not support offline transactions when there is no network access to the EFT Client software installed on servers at the secure data centres but this can be mitigated through a resilient network architecture that offers failover at all points, including router, network and server.

## The Vodat Managed Payment Service

Vodat International supplies secure private managed networks for retailers which it uses to provide retailers added value services that exploit the benefits of secure high speed networks.

Vodat already carries card payment authorisation transactions through its secure MPLS network and data centres for many of its retail customers. To provide such services Vodat has had to demonstrate that it is capable of handling card payment transactions securely. Vodat is a PCI DSS validated service provider and its Information Security Management System is certified as complying with ISO 27001.

Vodat is well placed to provide a managed payment service for retailers looking to remove cardholder data from their own systems in response to PCI DSS. This fundamental change in the requirements has led to many retailers looking for payment solutions that are independent from a POS solution and, thereby, removing the need to replace POS and payment solutions at the same time. These retailers want a payment solution that can be coupled to any POS solution through a simple exchange of non sensitive data.

To launch a managed payment service, Vodat searched for partners that offered solutions that could take advantage of its secure private managed network and offer retailers a flexible solution for the future. Vodat selected the G8way EFT Client from Smart Technology Solutions as our **EFT Client** and the Authentic payment gateway from Alaric as our **EFT Server**. The combination of these two solutions allows Vodat to offer retailers the required flexibility.

The **STS G8way EFT Client** was selected because it:

- Allows the business logic processing to be migrated away from the terminal firmware, POS hardware and back office servers to centralised servers
- Supports different solution architectures, including allowing the business process logic to be installed on the POS hardware and back office servers in addition to centralised servers and, thereby, is able to support a migration from store based architectures to a centralised architecture
- Includes the **STS SmartNS framework**, a “Smart Card Enablement Layer” that supports and integrates smart card applications through any point of interface to any business system
- Includes **STS Emvelink** a software-based EMVCo certified Level 2 Kernel for Chip and PIN transactions that supports over 30 payment devices (PEDs) from the leading payments hardware manufacturers
- Can be loosely coupled to POS applications through a simple XML or Java client interface whether installed locally or centrally.

The **Alaric Authentic payment solution** was selected because it:

- Provides a high performance, reliable, secure and scalable switch to route all forms of card transactions to multiple acquirers
- Includes the **Alaric Message Mapper**, a high performance, point-and-click configurable message transformation engine that allows the solution to be configured easily to accept new card types and add their associated acquirers
- Is the high-end open systems switch product of choice for tier one institutions and has already been delivering bank-strength cryptographic security for ATM customers for the past decade using the **Alaric Key Management Subsystem**

- Enables other on-line transactions as well as payments, including loyalty, gift/store value cards and DCC, either by storing balances or lookup information locally or by connecting to host or third party systems
- Provides comprehensive settlement and settlements reporting capabilities through Oracle database allowing tight bank settlements deadlines to be met reliably
- Uses secure web services over an inherently Service Oriented Architecture (SOA) platform to provide services to the retailer securely and flexibly
- Is a multi-channel central platform that is capable of managing payment and real-time transactions from integrated POS, standalone POS, ATMs, self checkout, kiosk, fuel, internet, mobile and other points of customer interaction
- Is fully flexible in terms of transaction types and transaction evolution, such that adding new online transaction types (e.g. direct CRM offers at the point of sale in real time or biometric fields to the transaction message) will be less costly, lower risk and faster to implement.

In partnership with STS and Alaric, Vodat has developed a managed payment service that:

- Uses applications certified under **PA-DSS** to provide an end-to-end solution from a **PCI DSS** compliant service provider using an **ISO 27001** certified Information Security Management System
- Handles cardholder data in a segmented part of the retailer's network
- Removes sensitive cardholder data from the retailer's POS and systems
- Allows loose coupling to POS solutions through a simple data exchange using a Java or XML client interface
- Provides POS solution independence
- Provides payment device (PED) independence
- Can support any card and any acquirer.

As a provider of secure private managed networks for retailers, Vodat is perfectly placed to deliver a second generation card payment solution that takes advantage of thin client architecture. Through managing proactively the secure MLPS networks on behalf of its retail customers, Vodat is able to ensure that the networks offer high levels of availability.

The combination of high availability secure private managed networks with the STS G8way EFT Client allows the Vodat Managed Payment Service to deliver a card payment solution where the EFT Client can be installed at its secure data centres, as set out in Option 5 of the Architecture Options for Delivering a Card Payment Solution section of this paper.

Where Vodat does not manage a retailer's network the flexibility of the Vodat Managed Payment Service allows the G8way EFT Client to be installed on a secure local server at the retailer's stores, as set out in Option 4 of the Architecture Options for Delivering a Card Payment Solution section of this paper, or Vodat can provide a secure link to the existing provider's network to allow G8way to be installed at the secure data centre, as set out in Option 5.

Where a retailer is unable to replace its existing locally connected PEDs with IP connected devices, the Vodat Managed Payment Service can offer these retailers the STS G8way EFT Client installed on the POS, as set out in Option 3 of the Architecture Options for Delivering a Card Payment Solution section of this paper.

In summary, the Vodat Managed Payment Service offers flexible architectures with the EFT Client installed:

1. At the Vodat secure data centre
2. On a secure local server at the retailer's stores
3. On the POS to provide a transition from the a retailer's current payment solution architecture to the above architectures
4. In any combination of the above three architectures.

The Vodat Managed Payment Service delivers a flexible solution and a roadmap for retailers wanting to remove their POS from the PCI DSS scope. It is designed to meet today's PCI security standards and it provides a strong platform to accommodate future changes in the standards while allowing the retailer to be virtually POS and PED independent. It offers a transition path for those retailers that are unable to replace their existing locally connected PEDs immediately or, as we say, it gives the retailer ***"POS exemption without PED redemption."***

## Glossary

| Term                          | Definition                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Cardholder</b>             | Customer to whom a payment card is issued to or any individual authorised to use the card.                                                                                                                                                                                                                                                                                                  |
| <b>Chip and PIN</b>           | A payment transaction that is protected a combination of chip card and a personal identification number (PIN).                                                                                                                                                                                                                                                                              |
| <b>EFT Client</b>             | Application that manages the messages between the PIN entry device (PED) and the EFT Server.                                                                                                                                                                                                                                                                                                |
| <b>EFT Server</b>             | Payment engine / switch installed at the secure data centre to manage authorisations, submit settlement files and provide transaction enquiries and reporting.                                                                                                                                                                                                                              |
| <b>EMVCo</b>                  | Organisation responsible for type approval processes, which include terminal compliance testing, as well as Common Core Definitions (CCD) and Common Payment Application (CPA) card compliance testing. These testing processes ensure a single terminal and card approval at a level that will allow cross payment system interoperability through compliance with the EMV specifications. |
| <b>EMVCo Level 1 Firmware</b> | Application firmware that is certified as satisfying the test requirements and test cases for the terminal chip card interface (Level 1). Level 1 Type Approval tests compliance with the electromechanical characteristics, logical interface, and transmission protocol requirements defined in the EMV Specifications.                                                                   |
| <b>EMVCo Level 2 Kernel</b>   | Application Kernel that is certified as satisfying the test requirements and test cases for the payment application (Level 2). Level 2 Type Approval tests compliance with the debit/credit application requirements as defined in the EMV Specifications.                                                                                                                                  |
| <b>IP</b>                     | Acronym for "internet protocol." Network-layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite.                                                                                                                                                             |
| <b>ISO 27001</b>              | Information Security Management Standard that specifies a management system that is intended to bring information security under explicit management control.                                                                                                                                                                                                                               |
| <b>MPLS</b>                   | Acronym for "Multiprotocol Label Switching." A mechanism in high-performance telecommunications networks which directs and carries data from one network node to the next. MPLS makes it easy to create "virtual links" between distant nodes. It can encapsulate packets of various network protocols. The technology of choice for delivering secure private networks..                   |
| <b>PA-DSS</b>                 | Acronym for "Payment Application Data Security Standard. The PCI security standard for software developers and integrators of applications that store, process or transmit payment cardholder data as part of authorisation or settlement.                                                                                                                                                  |
| <b>PCI</b>                    | Acronym for "Payment Card Industry."                                                                                                                                                                                                                                                                                                                                                        |

| Term                           | Definition                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PCI DSS</b>                 | Acronym for “Payment Card Industry Data Security Standards.” Applies to any entity that stores, processes and/or transmits cardholder data.                                                                                                                                                                                                                                           |
| <b>PCI Security Standards</b>  | Technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder payment data. PCI standards include PCI Data Security Standards (PCI DSS), Payment Application Data Security Standards (PA-DSS) and PIN Transaction Security (PTS).                                                                                          |
| <b>PED</b>                     | Acronym for PIN entry device.” In the context of this report, used to describe payment devices that include chip card readers and PIN entry keypad.                                                                                                                                                                                                                                   |
| <b>PIN</b>                     | Acronym for “personal identification number.” Secret numeric password known only to the user and a system to authenticate the user to the systems. A PIN is used in EMV chip cards where the PIN replaces the cardholder’s signature.                                                                                                                                                 |
| <b>POS</b>                     | Acronym for “point of sale.” In the context of this report, it is the hardware and/or software used by the retailer to process a sale of goods. Otherwise known as a till or cash register.                                                                                                                                                                                           |
| <b>Private Network</b>         | Network established for an organisation that uses private IP address space. Private network from public networks should be properly protected with the use of firewalls and routers.                                                                                                                                                                                                  |
| <b>Private Managed Network</b> | Private network that is managed by a third party service provider.                                                                                                                                                                                                                                                                                                                    |
| <b>PTS</b>                     | Acronym for “PIN Transaction Security.” The PCI security standard for the PIN based payment chain including PIN entry devices, other physical devices and non device types (e.g. HSMs) that play a role in PIN transaction security.                                                                                                                                                  |
| <b>Public Network</b>          | Network established and operated by a telecommunications provider, for specific purpose of providing data transmission services for the public networks. Data over public networks can be intercepted, modified and/or diverted while in transit. Examples of public networks in scope of the PCI DSS include, but are not limited to, the internet, wireless, and mobile technology. |
| <b>SOA</b>                     | Acronym for “Service Oriented Architecture.” A software architecture where functionality is grouped around business processes and packaged as interoperable services.                                                                                                                                                                                                                 |
| <b>SSL</b>                     | Acronym for “secure sockets layer.” Cryptographic protocol that provides security for communications over networks. Allows client/server applications to communicate across a network in a way designed to prevent interception and tampering. TLS protocol is an enhanced version of SSL.                                                                                            |
| <b>TLS</b>                     | Acronym for “transport layer security.” Cryptographic protocol that provides security for communications over networks. Allows client/server applications to communicate across a network in a way designed to prevent interception and tampering. TLS protocol is an enhanced version of SSL.                                                                                        |