



Merchant Value Proposition Tyro's Internet Payment Architecture

The attached White Paper documents the old EFTPOS banking world versus the new Tyro IP EFTPOS world. It is somewhat technical, so here are the business highlights. In a nutshell, we eliminate the existing legacy payment system network, its associated problems, limitations and costs. Instead we are using the Internet Protocol network (public or private). The key advantages of the Tyro IP EFTPOS solution are:

Elimination of the PCI-DSS compliance issue

Since with Tyro the sensitive card holder and transaction data never touches the merchant's space, he is not exposed to data breaches and not to the risks, complexities and costs that the increasingly excruciating data security standards impose on merchants. Visa and MasterCard have started pushing this agenda this year in a big way.

Elimination of EFTPOS availability issues

Since the Tyro transaction processing uses state-of-the-art, resilient and redundant public or private core networks, the merchant is not exposed to the risks of incumbent, single point of failure proprietary networks. Tyro plans to migrate this year to a live-live data centre infrastructure eliminating acquirer failure. That means raising dramatically the bar for the industry.

Elimination of transaction speed delays

Since Tyro uses high physical interconnect speeds, high network (& payment terminal) equipment processor speed and memory capacity and always connected communication with the transaction switch, authorisation, transacting and reporting speed have come down substantially. Tyro maintained sub three seconds processing times all through the Christmas trading period.

Elimination of infrastructure and communication costs

The use the existing IP network under the merchant's or a service provider's management eliminates the risk, complexity and costs of old and duplicate network equipment, of dedicated communication lines (PSTN dial-up or Argent) and of an entire software middleware layer (PC-EFTPOS or Quest).

We work by elimination. We make it simple. With less to operate and fail, we offer a solution that is more secure, simple to use, fast and less expensive than any other acquiring institution can offer. It is suitable for the small merchant with a single ADSL line to the big merchant with a complex MPLS based payment network.

MoneySwitch Limited
t/a tyro payments
abn 49 103 575 042

125 york street
sydney nsw 2000
p+61 2 8907 1700
f+61 2 8907 1777
h+1 300 966 639
www.tyro.com

**Comparing Legacy Payment Systems
With
Tyro's Internet Payment Architecture**

By

**Andrew R Rothwell
CTO & Co-Founder,
Tyro Payments.**

This document provides an overview of a merchant's typical, existing, legacy payment system network for processing card transactions, its associated problems and limitations. It then describes how Tyro can integrate its own acquiring system into a merchant's corporate network, relieving the merchant of all PCI compliance issues, improving reliability and speed of transaction processing, and leveraging the inherent scalability of the corporate network to eliminate existing payment infrastructure costs.

Version 1.1

January 20th, 2010.

1 Introduction to Payment Networks

Historically, payment networks for merchants were designed, implemented and operated in several ways, always as an adjunct, separate service to any existing corporate network/systems. Network technologies such as PSTNs (public switched telephone networks), serial lines, modems, protocol converters, payment terminal (or rather transaction) aggregation servers and x.25 switches were commonplace.

Today's modern merchant network is designed and implemented using Internet (IP) technology such as routers, firewalls and switches; which carry an array of different traffic. As will be shown, the task of forwarding card payment transactions from merchant store locations to a modern acquirer such as Tyro, becomes simpler: IP EFTPOS transactions become just another type of traffic to be carried across the merchant's (existing) IP network.

Both legacy and IP transaction forwarding networks are described below, highlighting differences in equipment required, costs, reliability, speed and operation.

2 Common Legacy Payment Networks

The two most common legacy network designs involve the use of dedicated networking equipment to forward transactions from the merchant's EFTPOS device to the acquiring bank.

One style of legacy connectivity uses a single dedicated network connection from the merchant store (often connecting multiple EFTPOS devices) to the payment provider, which may be a 3rd party payment gateway or the merchant's acquiring bank. Such network connectivity is generally provided using Frame Relay, ISDN, or x.25 in the past. This type of network is further described and illustrated in section 2.1 below.

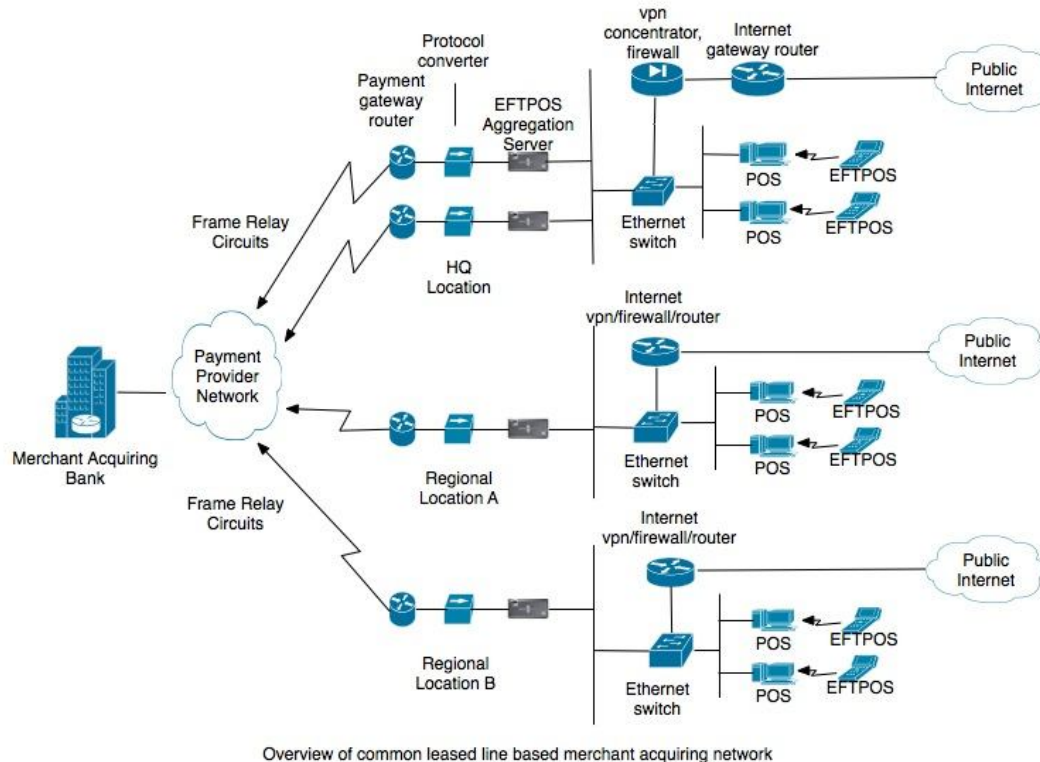
A second style of legacy connectivity uses multiple PSTN based network connections, one from each EFTPOS device in the merchant store to the payment provider. Such connectivity is provided using serial modems (either built-in to the terminal or external). This type of network is further described and illustrated in section 2.2 below.

2.1 Leased Lined based Payment Networks

Leased line payment networks generally, but not always, have the property that they aggregate transactions from multiple EFTPOS devices in the merchant store and forward them down a single dedicated network connection to the payment provider. Very frequently multiple network elements are needed to forward transactions in this environment. The diagram below illustrates the typical network devices used, including EFTPOS transaction aggregation gear.

It is fairly obvious that the networking equipment required to support a leased line design adds to the overall cost, complexity and operation of the whole merchant network. Furthermore the services of a 3rd party payment gateway provider are generally required, adding further cost. Increasing the number of network elements in

the transaction forwarding path clearly increases the potential for reduced reliability of the merchant payment network.



In order to provide redundancy in leased line networks for stores with a corporate network, the head office location may implement redundant links to the payment provider, while each regional location employs a single leased line to the payment provider. Payment network redundancy for regional stores may be provided by:

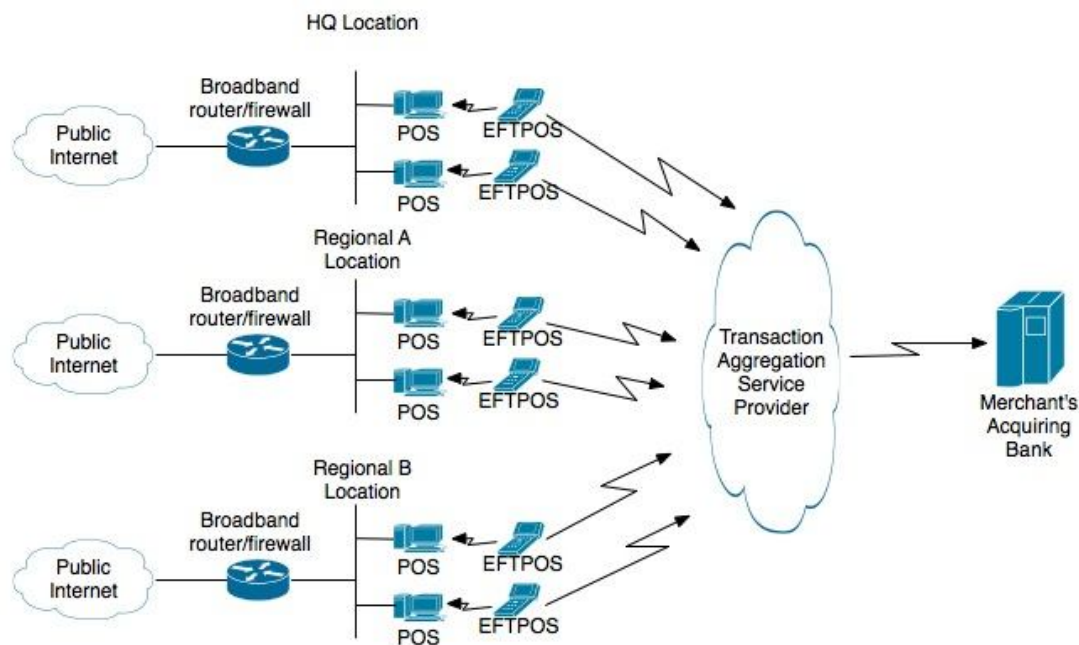
- a) Routing payment transactions through the corporate network to the head office location, where they then are forwarded through (one of two) redundant links to the payment provider. Or,
- b) Routing payment transactions across a dial backup link to the head office location, if the corporate network failed.

2.2 Dialup based Payment networks

In this scenario, each EFTPOS device connects via the PSTN to a payment provider, who may be a 3rd party gateway (such as Telstra's old TranSend operation) or the acquiring bank and its own EFTPOS transaction aggregation systems. The diagram below illustrates a typical merchant payment network using dialup technology. (Note that recently manufactured EFTPOS devices include built-in modems, while older equipment often requires an external serial modem to connect to the payment network.)

It is clear to see from the diagram below, that while a EFTPOS device requiring a single PSTN connection for a single merchant may represent a small cost of accepting cards; many PSTN connections certainly do not represent a small cost in the case of

multiple EFTPOS devices per store. And if a merchant has a number of stores the cost becomes onerous. Many medium to large merchants chose to employ the leased line network described above, to avoid such expense.



Overview of common dialup or ISDN based merchant acquiring network

Providing fault resilience in dialup networks such as this is difficult, since there is a single PSTN line directly connecting each payment terminal. The assumption in this network topology is that a single line will fail. If the transaction aggregation provider fails however, all EFTPOS processing ceases.

3 MPLS and Internet based Payment Networks

Merchants of almost any size these days are beginning to recognize the benefits of implementing an IP based (corporate) network. Many different services can be carried across the IP network, e.g. email, web browsing, real time POS inventory updates, voice over IP (VoIP), security alarm and streaming video, and now EFTPOS transactions.

Some of this traffic is highly sensitive, requiring protection from prying eyes. Private networks built on Internet Protocols such as SSL, IPsec and MPLS all provide such protection.

Small merchants can choose to implement a private IP network using standard VPN (virtual private network) technology such as SSL or more commonly IPsec, to connect all stores.

Medium to large size merchants can choose to implement a private IP network to connect all their stores using another technology known as MPLS (multi protocol label switching). For these merchants MPLS provides better scalability from operational, (traffic) management and therefore cost saving perspectives.

In both MPLS and (VPN) Internet based networks, the need to distinguish and process network traffic such as EFTPOS is crucial. Fortunately network traffic can be distinguished and prioritized, so that important traffic such as EFTPOS receives highest priority for forwarding; e.g. over and above VoIP, POS traffic, email, etc.

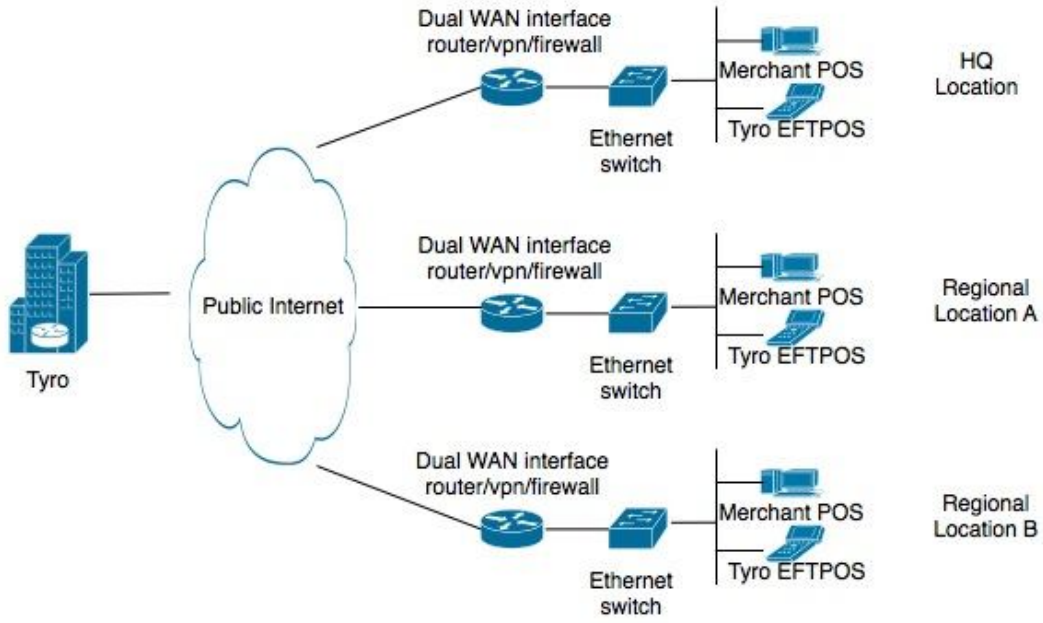
3.1 Public Internet based Payment Networks

For smaller merchants, implementing a single store or store-to-store network is as easy as buying and installing an integrated broadband switching router, and connecting in-store computers to this device. As previously mentioned, building private IP networks for store-to-store communications may be accomplished using SSL or IPSec. These features are often found in high-end VPN enabled SOHO routers, costing only a few hundred dollars.

Being able to differentiate and provide differing quality of service (QoS) to each type of traffic (VoIP, email, EFTPOS) passing through the VPN is possible, but again, dependent upon the type and model of broadband router purchased.

From the diagram below it is plain to see that when using IP enabled EFTPOS equipment such as Tyro's, the requirement for extra payment networking equipment becomes redundant. The existent IP (broadband) network is leveraged to forward transactions from the merchant's Tyro terminal to Tyro's data centre(s).

Providing non-stop transaction processing across the Internet is improved if merchants use broadband router equipment that supports dual WAN interfaces, e.g. 1 primary ADSL interface and 1 secondary 3G (mobile) interface. Such routers should support auto failover from primary to secondary. When the primary network interface again becomes available, the router should automatically switch back to using this. Such automatic operation alleviates the merchant from having to understand when and how to manage his network (equipment), if his primary network connection becomes unusable.



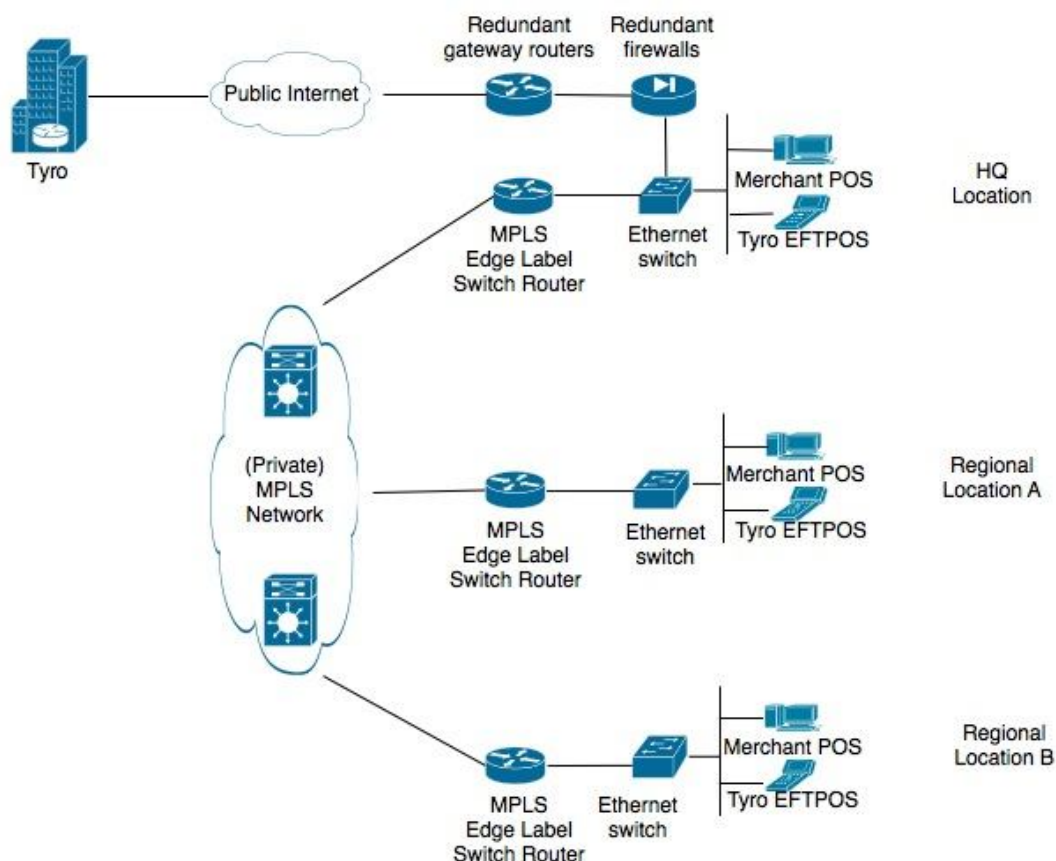
Overview of Internet based merchant network using Tyro acquiring system

3.2 MPLS based Payment Networks

Multi-Protocol Label Switching (MPLS) was originally presented as a way of improving the forwarding speed of routers but is now emerging as a crucial standard technology that offers new capabilities for large-scale IP networks. Traffic engineering, the ability of network operators to dictate the path that traffic takes through their network, and Virtual Private Network support are examples of two key applications where MPLS is superior to any currently available IP technology.

MPLS networks are composed essentially of two parts: Edge Label Switch Routers (ELSR) residing in the merchant's store network, which connect to Label Switch Routers (LSR) that reside in the (internet) service providers core network. The merchant's ELSR is responsible for forwarding merchant IP traffic, using any configured traffic engineering policies onto the MPLS service provider core network via the LSR, for switching to other stores in the merchant network.

From a transaction forwarding perspective, with respect to the Tyro payment terminal and Tyro's data centre, the MPLS network is completely unseen. It simply forms part of the network over which transactions flow. The following diagram illustrates a simple MPLS network.



Overview of MPLS based merchant network using Tyro acquiring system

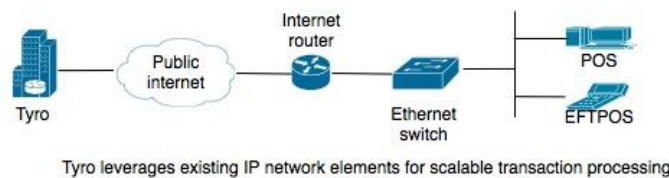
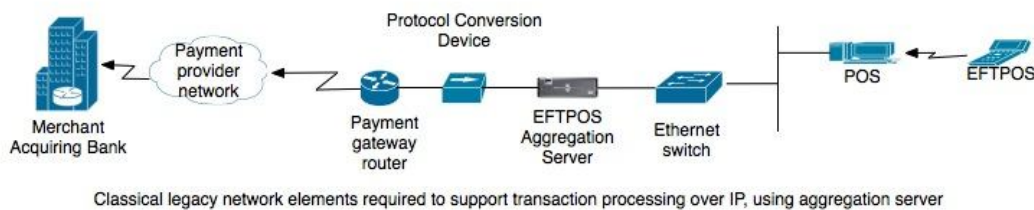
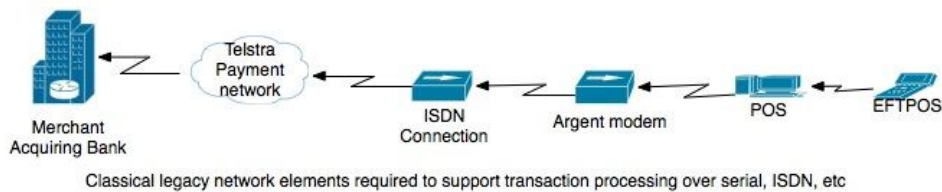
Note however, to ensure reliable and fast transaction forwarding (relative to all other traffic flowing through the merchant's network), the MPLS routers must be

configured such that financial transaction traffic receives priority in handling and forwarding, relative to all other traffic. Diffserv QoS can provide such functionality.

MPLS networks can be easily designed to support fault tolerant operation, by providing dual network interfaces and redundant paths through the MPLS network.

4. Transaction Forwarding Paths: Legacy versus Internet

We have described various legacy and modern network communication technologies, focusing on issues such as scalability, availability, etc. In this section we briefly revisit the transaction forwarding paths from each. The diagram below outlines a few key forwarding paths.



Transaction path comparison: Legacy systems versus Tyro Internet system and required network elements

Clearly both legacy paths are longer, adding extra equipment and complexity into the network. The additional equipment obviously adds to increases in transaction processing times, lowers overall payment network reliability, increases operational complexity and management, and ultimately cost.

Conversely, the Internet path contains less equipment, giving rise to faster transaction authorization (aka round trip) times, higher network reliability, lower operational complexity and lower cost.

In the dialup and leased line networks, transactions can take considerable time to be processed, sometimes upwards of 15 to 20 seconds. This is due to various network and equipment issues, such as:

- a) The nature of the underlying communications method being used. For a single authorization, several other unseen messages are exchanged to complete the

transaction. Typically a “connect” request is made at the data link layer (modem) to the remote location (payment gateway, acquiring bank), followed by sending of the authorization, then receiving a response, and finally “disconnecting” the modem from the remote location. This is done for each and every transaction. Of these four network operations, the “connect” request was generally responsible for consuming the largest amount of time.

- b) Older network equipment was generally constrained with regard to processor power and memory availability, so the ability to process the transactions at speed was limited.
- c) The network communications physical layer, i.e. the wiring and circuitry transmitting and receiving the transactions operated at slower speeds, typical modem speeds for EFTPOS traffic operate at 9.6Kb/sec.

In today’s payment networking world, especially Tyro’s, these three performance limitations are removed, to wit:

- a) Tyro’s payment application does not use the “connect”, “send”, “receive” and “disconnect” method for processing each transaction. Instead a (SSL session and TCP) “connect” is issued at terminal startup time, and transaction processing is composed of (SSL and TCP transmit) “send (authorization)” and “receive (response)” messages. When the terminal is shutdown a (SSL session and TCP) “disconnect” is issued. Fewer exchanged messages between the terminal and the bank equates to speedier authorization times.
- b) Tyro uses IP based terminal equipment that use dual processors, and have a large memory footprint, so transactions can be created, authenticated, encrypted and transmitted in milliseconds. Furthermore all the intermediate networking equipment employs high-speed processors (and very frequently ASICs) and large memory footprints to process network traffic at high speed.
- c) Also, The physical interconnects between networking equipment also operate at much higher speeds, so transactions are forwarded at much higher speeds across the Internet than was the case for legacy systems and networks. For example, ADSL modems that connect a merchant’s in-store broadband router to their service provider operate at up 22Mb/sec.

It’s worth noting, that the average response time (round trip time) for an authorization request originating from a merchant’s Tyro terminal, to the local domestic banks (for credit or debit cards) is about 2.5 seconds.

5 PCI DSS Compliance

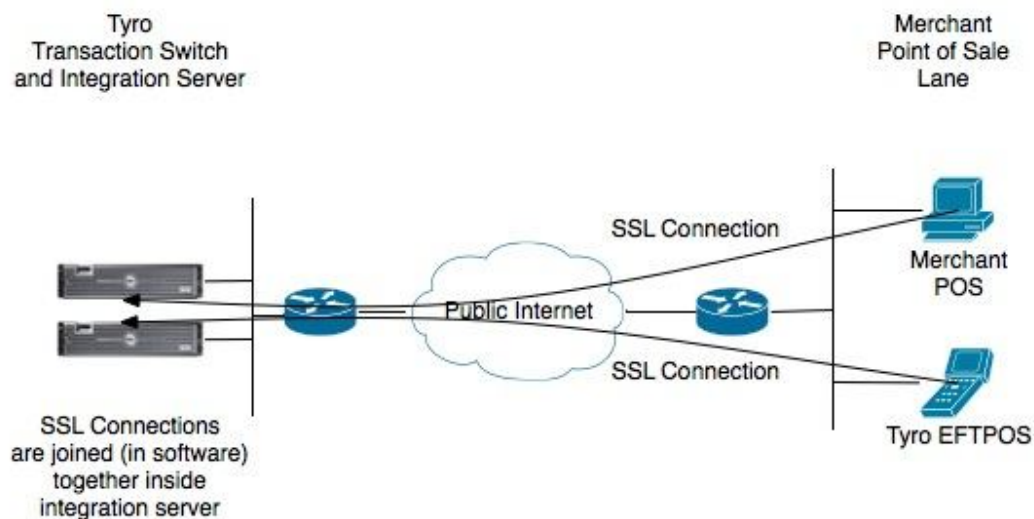
In the legacy scenarios mentioned above, all cardholder data (most especially track 2 data) that is captured and transmitted from the EFTPOS device toward the acquiring bank is done so unencrypted.

There are effects underway (being championed by the technical security group at APCA) to enforce all future EFTPOS devices to encrypt cardholder data, however this likely will take quite some time, and will potentially require a forklift upgrade of all EFTPOS equipment, for complete replacement.

While this may not be seen to be problematic when the EFTPOS device is directly connected to acquiring bank infrastructure (via PSTN or leased line), the same is not necessarily true if EFTPOS traffic passes through intermediate systems such as POS and/or transaction aggregation servers. This contravenes basic PCI DSS cardholder rules, which states that all cardholder data must be fully protected at all times.

In an integrated POS and EFTPOS environment, unencrypted EFTPOS transactions that arrive at the POS for forwarding may be intercepted by rogue software, recorded and retransmitted to an unauthorized location/organization for fraudulent use, completely unbeknown to the merchant. (Similarly, it is not difficult to insert an inline device that “sniffs” transactions originating from a serially connected EFTPOS device, and have them transmitted wirelessly to an unauthorized location.)

At Tyro, this situation can never occur. It cannot because the POS and EFTPOS device both communicate with each other via Tyro’s transaction switch and integration server, using two-way authenticated SSL sessions. These devices never allow any form of sensitive cardholder information to be exchanged between EFTPOS and POS devices. The only traffic flowing between these devices are simple requests for payment authorization, request and device status updates, and payment responses with detail for receipt printing on the POS printer. This is shown diagrammatically below:



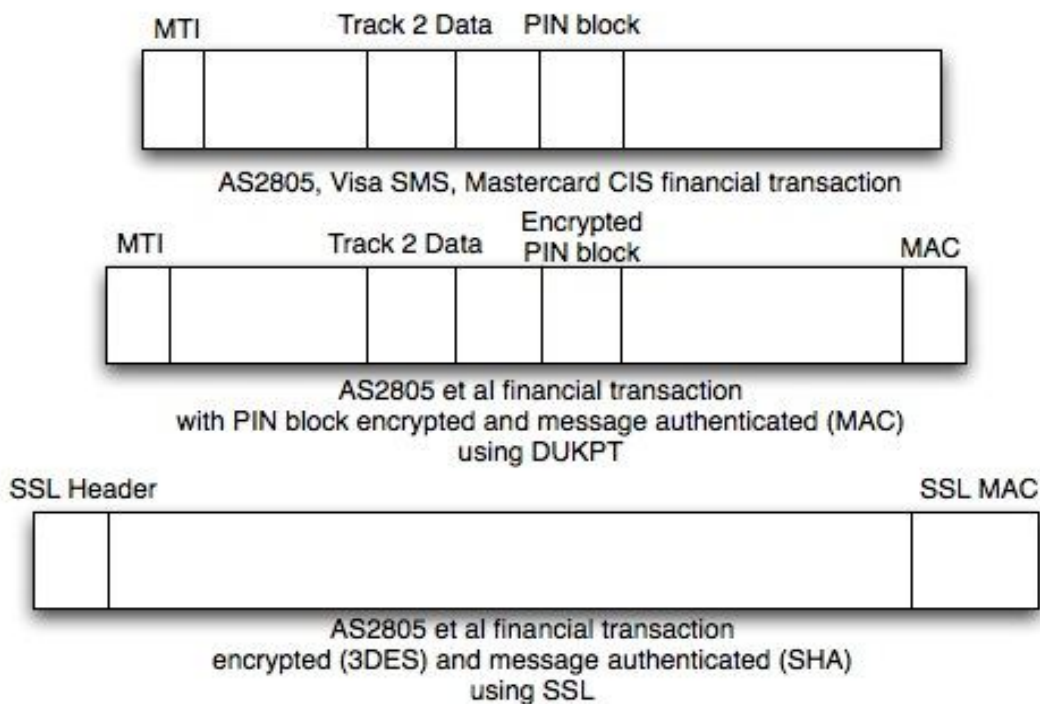
Overview of Merchant POS and Tyro EFTPOS terminal integration architecture

Tyro’s data centres which house the transaction switching and database systems have been through rigorous certification processes including APCA’s PIN audit and the

PCI DSS certification (which was run under the supervision of Visa). Tyro was the first financial institution in Australia to be granted PCI DSS certification.

Tyro's payment terminals have also been PCI PED certified.

All Tyro transaction traffic is forwarded from the payment terminal through the merchant and service provider networks to Tyro using two-way authenticated SSL sessions. Additionally all financial transactions originating in the payment terminal and forwarded through the SSL session are MAC'd (message authenticated), and PIN blocks are encrypted using DUKPT and 3DES with double length keys. So there are two layers of protection afforded financial transactions in Tyro's payment network. The following diagram illustrates this.



Finally, the separation of POS and payment terminal via the Tyro integration server and transaction switch, and the double protection (authentication and encryption) of financial transactions make the Tyro payment network ultra secure.

6 Conclusions

Tyro payment networks use existing merchant and public IP network infrastructure (merchant and service provider) to forward transactions to Tyro's data centres. Because of this, we can leverage the inherent security, scalability, reliability and speed of these networks. Over and above this, Tyro adds its own mechanisms to protect cardholder data, providing truly world-class security.

All of this makes Tyro payment networks secure, simple to use, fast and less expensive to operate than that provided by any other card acquiring institution in Australia.