Secure Payments Guide

- Hosted solution
- Point to point encryption
- Tokenisation

pxp

How to reduce data security liability

Reduce data liability · Hosted solution

· De-scope PCI
· P2PE application & solution

Accepting card payment is a necessary part of running a customer-facing business. But storing, processing and transmitting card data comes with risks. Our hosted point to point encryption (P2PE) and tokenisation services help you take card payment without taking card data, thereby reducing your liability and PCI scope.

PXP's managed security services help all types of businesses reduce their liability and are designed around four key principles: · Secure all sensitive consumer data · Allow the merchant to drive the customer payment experience · Remove liability from the merchant in the case of a breach · Reduce costly overhead to the payment infrastructure

PXP's managed security services help merchants reduce their liability.

pxp

Point to point encryption (P2PE)

Criminals want card data, preferably in the clear so they can monetise it. They write malicious software to harvest data from point-of-sale (POS) applications. Encrypting data from the moment it enters your systems means you never see sensitive cardholder data in the clear. This helps reduce your risk in the event of a breach, the associated costs (e.g. lost revenue, reputation, trust), plus your PCI scope. PXP offers P2PE as a managed service for customers either as an application or as a full solution. Both have been tested by trained P2PE assessors retained by the Payment Card Industry Security Standards Council (PCI SSC) against the standard.

P2PE application

This approach provides assurance that the application is encrypting the transaction on the PIN entry devices (PED) using suitably strong encryption methods. The transaction is only decrypted once it reaches PXP's internal systems. Providing there is no other interaction with the card or the PED, there will be no clear card data anywhere on your systems. However, the P2PE application cannot tell if PIN entry devices have been tampered with prior to installation. Nor does it guarantee that card data is not being captured elsewhere in your system. Or minimise the time a compromised device remains in operation.

P2PE solution

This is a full end-to-end service and includes business processes for securing your terminal estate. It includes provisions around terminal deployment, security, maintenance and storage (sometimes known as 'chain of custody'). You can be assured that the PIN entry device has not been tampered with prior to installation, and that it has been installed securely by a trained engineer. However, the operational overhead around time, cost and expertise is higher than for the P2PE application.

P2PE helps reduce your risk in the event of a breach, the associated costs as well as your PCI scope.

pxp

Tokenisation

Tokenisation replaces sensitive card data with a token, which can be used across various front- and back-end systems instead of the real card data. PXP's tokenisation works across channels, countries and brands/ franchisees in a business group. It can also be activated retrospectively on stored card details. This simplifies compliance with data security requirements, and also delivers operational, cost and marketing efficiencies.

- Format preserving tokenisation with either 16- or 19-digits means you can use existing business applications and databases that store card numbers without modification, preserving existing staff and customer processes.

- Cross-channel tokenisation works for all types of transactions (face-to-face, remote, sales, refunds, pre authorisations etc.), to power and protect an omni-channel strategy.

- Tokenisation across sub-brands or franchises in a business group helps deliver operational and cost efficiencies.

- Individual transactions or batches of stored card details can be tokenised and protected retrospectively without completing a transaction.

- Compatibility with any front-end business application interfacing to the PXP API, including the Micros Opera FIAS interface for property management systems, makes our tokenisation easy to implement.

Customers are seeing extra benefits around the operational, cost and marketing efficiencies of tokenisation. These can be as significant as the security benefits — sometimes more so.

pxp

Top tips to keep your customers' data safe

Here are our five top tips to help keep your customers' card data safe while you focus on running your core business.

1. Use a hosted solution

Outsourcing payment security to a trusted partner as a fully managed, hosted solution saves you time in keeping up with industry standards. It saves the cost of training your own experts and the investment your provider makes for its client base as a whole.

2. Deploy point to point encryption

With P2PE, your customers' card data is encrypted directly on the PIN entry device. It remains encrypted until it reaches our secure data centre, so your terminals and systems never see any sensitive data in the clear. This minimises the impact of a data security compromise.

3. Tokenise sensitive card data

Tokenisation replaces sensitive card data with a token which you can use across various front-end and back-end systems instead of the real card data. We store all your sensitive card data securely. Tokenisation offers data security benefits, plus operational, financial and marketing ones, too.

4. Reduce scope

Consider how you can change business processes to reduce PCI DSS scope. The savings in year one may be modest. However with no need to manage or maintain the activity in year two or three, the de-scoping exercise really begins to pay dividends.

Consider outsourcing payments on your e-commerce site to a third party via a hosted payment page, minimising the number of physical locations where card data is stored, and/or the number of staff who have access to it.

5. Focus on security rather than compliance

The goal of PCI DSS is to secure cardholder data. We advise adopting a matrix of measures. This includes detective, response and recovery controls to build operational resilience and accelerate post-incident recovery. While this may require cultural change and cross-company working, it helps emphasise that security is an ongoing process, not a one-off, annual exercise.

pxp