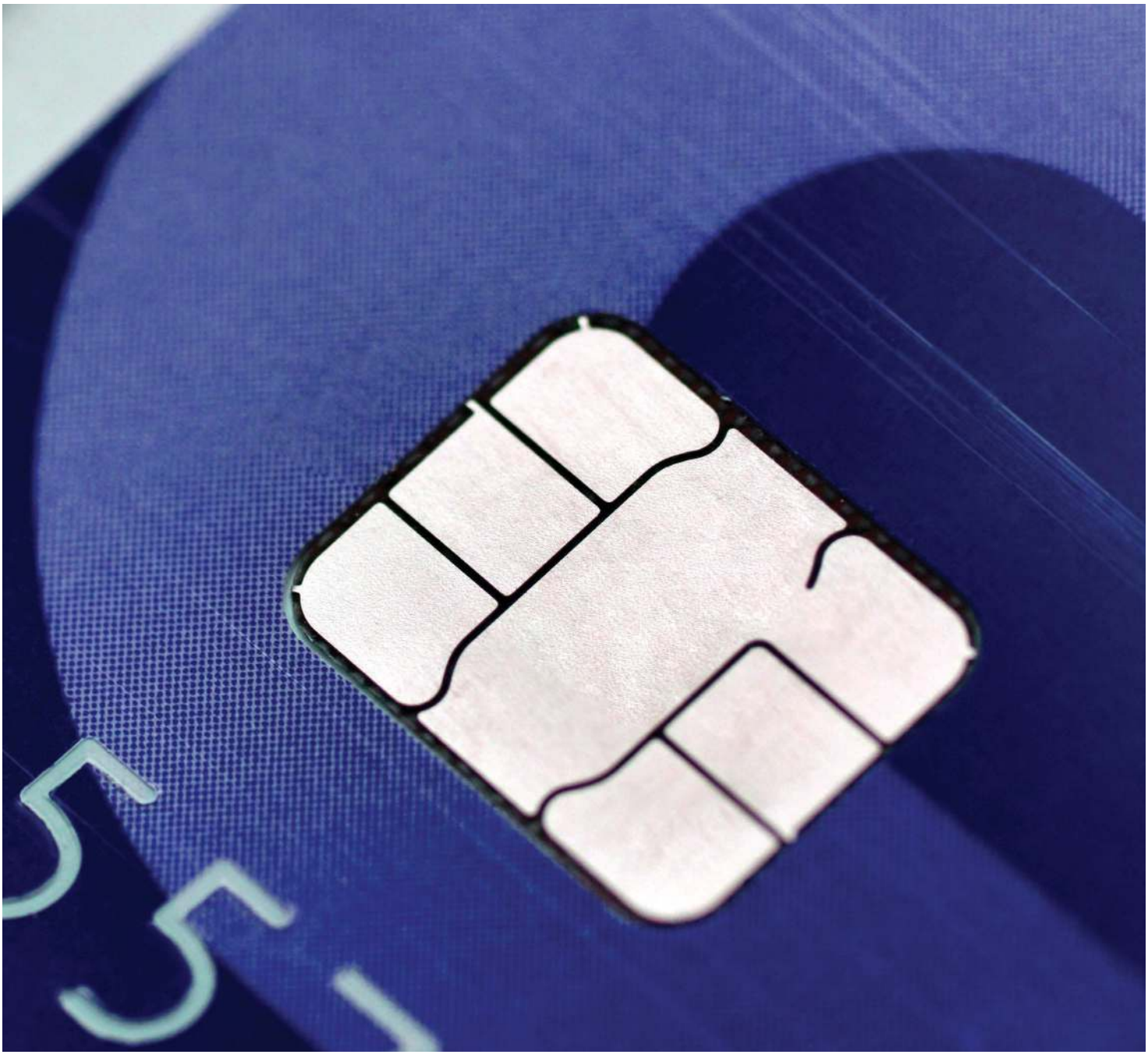
Point to Point Encryption (P2PE)

What you need to know about Point to Point Encryption (P2PE)

Michael Hopewell, Managing Information Security Consultant



Many businesses have heard about Point to Point Encryption (P2PE). Point of Sale vendors, service providers and others often mention its benefits to businesses: P2PE can reduce risk to payment card data by rendering it unreadable, minimise the number of systems and networks in scope for the Payment Card Industry Data Security Standard (PCI DSS) and simplify the process of achieving PCI DSS compliance.

However, due to a range of factors including misinformation and misunderstanding some businesses encounter issues realising those benefits. In this article, one of Sysnet's QSA (P2PE) and PA-QSA (P2PE) assessors, Michael Hopewell examines the common questions he is asked by merchant businesses about P2PE to address those factors to help you decide whether a P2PE Solution can help your business.

What is Point to Point Encryption (P2PE)?

Point to point encryption protects (encrypts) payment card data from the point of capture, such as when the card is read by a card payment terminal, until it reaches the secure decryption endpoint. Encryption is the process of converting the payment card data into an unintelligible form. The encrypted card data is of no value to anyone who may be able to intercept or steal the data, as they have no means to revert the data back to its original form.

Point to point encryption is the major feature of P2PE Solutions. These are PCI-approved solutions that have been independently assessed against the PCI Point-to-Point Encryption Solution Requirements and Testing Procedures (the P2PE Standard). A PCI-approved P2PE solution, as the PCI Security Standards Council (SSC) describes, includes not just point to point encryption but also "validated hardware, software, and solution provider environment and processes. Validation is done by a PCI-qualified P2PE assessor". The PCI SSC publishes the list of all validated and approved P2PE Solutions here. The PCI SSC also publishes lists of approved P2PE Applications and Components. These Applications and Components may be used as parts of a validated P2PE Solution. If your business is using only a P2PE Application or a P2PE Component listed by the PCI SSC that does **not** mean you are using a validated P2PE Solution.

Why should my business implement a P2PE Solution?

Using a correctly implemented, PCI SSC listed P2PE Solution in your business has the following benefits:

- **Lowers the risk of payment card data loss** - Data is encrypted at the point of capture and cannot be decrypted in your environment;
- **Reduces the extent of your PCI DSS assessment scope** - You can consider any connected Point-of-Sale system, your network and other components/devices sharing that network to be out of scope;
- **Simplifies PCI DSS compliance** – Fewer applicable PCI DSS requirements, simplified compliance assessment, and a potential reduction in the cost of maintaining compliance.

A P2PE Solution can ease the way to validating PCI DSS compliance for your retail environment; however, if your business also accepts card payments via other methods in the environment then validation of additional PCI DSS requirements will still be necessary.

My Point of Sale vendor / Terminal Provider tells me their solution uses End to End Encryption (E2EE) – is that the same as P2PE?

No, it isn't the same. Unless the provider's E2EE solution is a validated, listed P2PE Solution it is not the same and cannot offer the same benefits.

Many Point of Sale systems and card payment terminals make use of what is termed End to End Encryption (E2EE). E2EE follows the same principles as Point to Point Encryption – that is, encryption is used to protect the card data as it is sent from one endpoint (your business) to another endpoint (the solution provider or payment processor). However, in reality, your provider's E2EE solution could be significantly different to a validated P2PE Solution.

Some solutions claiming to be E2EE do not encrypt the payment card data immediately at the point of capture, within the card reader. The solution may instead rely on a payment application running on the Point of Sale system to encrypt the data before it is sent.

Some E2EE solutions only encrypt the card data as it is transmitted – the card data is protected only as it is sent across networks to the payment processor. As unencrypted card data may be present outside of the card payment terminal hardware, these types of E2EE solution do not offer anything close to the level of security for card data as a validated P2PE Solution.

There are other E2EE solutions that use the same technologies as those used in validated P2PE Solutions.[1] However, even if an E2EE solution uses the same encryption technologies, the solution cannot provide the same level of card data protection and security assurance as a validated P2PE Solution. There may be a weakness in any one of the elements that make up the E2EE solution – in the hardware or software used, in the solution provider's environment or in the processes used to implement and operate the solution.

The independent validation of a P2PE Solution provides assurance that there is a 'chain of trust' for the entire solution. Each element that makes up a P2PE Solution is tested against the requirements of the P2PE Standard. From the secure encryption environment deployed in your retail environment (the payment card terminal and its method of encrypting the card data at capture), the cryptographic operations (including injection of encryption keys into the terminals and key management), to the security of the decryption environment.

As those same elements in your provider's E2EE solution have not been independently validated, there is no way for you to know if your provider's E2EE solution is as secure as a validated P2PE Solution. As a result, you cannot achieve all of the same benefits with E2EE as you can with a P2PE Solution.

1 For example, they make use of approved PCI PTS card payment terminals and use the SRED (Secure Read and Exchange of Data) function in those terminals to encrypt data at the point of interaction with physical card.

I've been told I have P2PE card payment terminals (card reading devices) – does that mean I have a P2PE Solution?

My business uses PCI PIN Transaction Security (PTS) approved card payment terminals – does that mean I have a P2PE Solution?

The card payment terminal (card reading device) is only one component of a P2PE Solution. You may be able to find your terminals included in the list of PCI PTS devices supported by a PCI-listed P2PE Solution but that does not mean your deployment of those terminals is part of a validated P2PE Solution.

Your solution will only be a validated P2PE Solution if:

- It can be found as a P2PE Solution approved and listed by the PCI SSC
- The P2PE Solution includes only listed dependencies/components, your card payment terminals' make, model, hardware version and firmware version matches the PCI PTS listing for the 'PTS Devices Supported' by the P2PE Solution;
- The deployed card payment terminals are part of the validated P2PE Solution;
- The card payment terminals have been handled and installed in accordance with the approved P2PE installation and connection instructions;
- All device administration, payment card data related operations and cryptographic operations are entirely managed by the P2PE Solution;
- You have implemented all controls in the P2PE Instruction Manual (PIM) provided to you by the P2PE Solution Provider to make sure that the devices are secured throughout their lifecycle (receipt, storage, installation, use, movement, repair,replacement, decommissioning).

My card payment terminals (card reading devices) and terminal software matches a listed P2PE Solution – am I using a P2PE Solution without realising?

It is unlikely you are using a validated P2PE Solution without being aware of it. P2PE Solutions have strict processes for the secure deployment, installation and connection of the solution's card payment terminals. You would have to follow these processes when you received the terminals, for example to ensure they are stored securely before being deployed at your points of sale.

Each P2PE Solution provider is obliged to supply the business user with the solution's P2PE Instruction Manual (PIM). The PIM sets out your responsibilities to install and manage the card payment terminals correctly. If you have not received a PIM and have not implemented and are not following the instructions in the PIM, then you will not be using an approved P2PE Solution.

My Solution Provider tells me my deployment is not a valid P2PE Solution even though my payment terminals and terminal software match their listed P2PE Solution – what can I do?

It is possible that you are using card payment terminals (card reading devices) and terminal software, managed by a third-party solution provider, that match the details of a listed P2PE Solution but your deployment is not valid as a P2PE Solution.

This is usually because, although the solution provider offers a validated P2PE Solution, for your deployment the P2PE capable card payment terminals were not shipped, handled and deployed in a secure manner in line with the P2PE Standard and the P2PE Solutions approved processes. If the solution provider was not aware of your desire to implement a validated P2PE Solution, they may not have followed these strict P2PE requirements or have provided you with the P2PE Instruction Manual (PIM). If approved processes were not followed and/or the PIM has not been implemented and adhered to by you, your deployment will not be a validated P2PE Solution, eligible for the benefits outlined above.

If your deployment is not valid as a P2PE Solution, then you should ask your provider about your options to reset or re-birth your terminals. Your options could include sending your terminals back and getting them reset and re-shipped following the proper P2PE validated processes; or swapping your current terminals for fresh new ones, again sent to you following the proper P2PE processes.

Once the reset or re-birth is completed, and the requirements of the PIM implemented, your deployment will be a validated P2PE Solution.

Why do I still have to validate PCI DSS compliance when I am using a PCI approved P2PE Solution?

Implementing a validated P2PE Solution and operating it in accordance with the PIM, does not entirely remove the need for PCI DSS validation in your environment. Even though the payment card data is encrypted at the point of capture by the P2PE Solution, there are still potential risks to card data in your environment: risks at the encryption endpoints (your card payment terminals) and risks to any paper copy card data you may have in your environment. You still need to validate PCI DSS compliance to confirm that those risks are being addressed. The SAQ P2PE specifies the PCI DSS requirements that are applicable to merchants processing card payments via hardware payment terminals included in a validated P2PE Solution.

Can I use the SAQ P2PE to assess my PCI DSS compliance?

The SAQ P2PE is intended for SAQ-eligible merchants processing card payments via hardware payment terminals included in a validated, PCI-listed P2PE Solution. Even if your business is not eligible for self-assessment, you still may be able to use the SAQ P2PE to determine the applicability of PCI DSS requirements for your on-site assessment. If your environment fully meets all the eligibility criteria defined in the SAQ P2PE, consult your acquirer to find out whether you can use the SAQ P2PE as the reference for your assessment.

If you wish to assess your PCI DSS compliance using the SAQ P2PE you need to confirm you:

- Are using a validated PCI P2PE solution (per the PCI P2PE Program Guide).
- Do not store, process, or transmit any cardholder data on any system or electronic media (for example, on computers, portable disks, or audio recordings) outside of the payment terminal used as part of the validated P2PE solution.
- Do not store any cardholder data in electronic format. This includes verifying that there is no legacy storage of cardholder data from other payment devices or systems.
- Have implemented all controls in the P2PE Instruction Manual (PIM) provided by the P2PE Solution Provider.

What's involved in maintaining a P2PE Solution?

Implementing and maintaining your P2PE Solution requires your business to:

- Fulfil the controls set out in the PIM;
- Meet the PCI DSS requirements from the SAQ P2PE.

The PIM provides instructions and guidance on aspects such as maintaining a detailed and complete inventory of your payment terminals, installing and connecting the devices, securing devices in transit, physically protecting installed devices and taking steps to prevent tampering and unauthorised device substitution, etc. These business activities are critical to the overall security of the implemented P2PE solution.

The SAQ P2PE also includes requirements to make sure card payment terminals are physically protected in your environment. A summary of these requirements are as follows:

- Maintain an inventory of card payment terminals – You need both policies and procedures to make sure that you create and maintain an inventory of your terminal devices, across all locations. This means noting the make, model, location and serial number (or other unique identifier) of each device. A robust process must be in place to update this inventory when terminals are added, moved, replaced or decommissioned.
- Regularly inspect card payment terminals to check for tampering or substitution - Documented policies and procedures need to be in place, to make sure that your card payment terminals are periodically checked to make sure they have not been tampered with (e.g. card skimmer added) or substituted (e.g. for a bogus or compromised device). Your device inventory will help facilitate this check.

- **Make sure point of sale staff are aware of and know to report suspicious behaviour and indications of tampering or substitution** - Train all appropriate staff on how to verify the identity of terminal repair/maintenance personnel, to identify signs that a terminal might have been tampered with or substituted, to identify suspicious behaviour around card payment terminals, and to report suspicious behaviour or tampered/substituted devices.

Some PCI DSS requirements in the SAQ P2PE are applicable only if your business creates, handles or retains paper records (such as order forms, receipts, etc.) that contain payment card data, including the Primary Account Number (PAN). If you never write down, print or store paper records containing payment card data, these requirements can be marked Not Applicable (requirements 3.1, 3.2.2, 3.7, 9.5, 9.8, 9.8.1).

You will also need an appropriate security policy that explains to your staff how to use and protect the card payment terminals, in accordance with the PIM. It will need to define their security responsibilities, including how to report suspicious activities and security incidents. Your policies and procedures need to be supported by a security awareness programme, so that point of sale staff and others with responsibilities to fulfil the requirements of the PIM know what they need to do.

In conjunction with the P2PE Solution Provider, and other service providers you rely on, you should also define, agree and document a security incident response plan. This could encompass both a simple set of steps for point of sale staff to follow, as well as more detailed procedures for reporting and responding to specific incident scenarios so that all parties involved know their responsibilities.

The expected workload for implementing the SAQ P2PE requirements and maintaining your validated P2PE solution may surprise you at first. If you have a large terminal estate the requirements of the SAQ and PIM may take considerable time and effort to implement across all locations for all applicable staff. Once defined however, these procedures should be straightforward to operate and maintain, with regular reminders to point sale staff so that they remain vigilant.

Businesses may outsource some of your merchant responsibilities to third parties. Be cautious when doing this, it is often the case that the outsourced company is not fully aware of P2PE Standard or the amount of effort required to meet its requirements or that of the associated PIM. Typical items outsourced include physical security of the card payment terminals, reporting and tracking of the terminals and installation of the terminals. You should work with the third party provider to make sure that they have documented policies and procedures in place. Outsourcing the work does not outsource the responsibility to maintain compliance with the PIM and the SAQ P2PE requirements.

Conclusion

Businesses seek P2PE solutions for their scope reduction benefits, as P2PE solutions can be integrated with many of the common Point of Sale solutions while still allowing them to exclude the Point of Sale system and network from PCI DSS assessment scope.

As we have explained, having P2PE capable card payment terminals does not necessarily mean you have a validated P2PE solution or are eligible to complete an SAQ P2PE for your compliance assessment. To have a deployed, validated P2PE Solution you must have the combination of approved hardware, software, the P2PE solution provider's environment and processes (the listed P2PE solution), deployed in accordance with P2PE processes and maintained according to the solution's PIM.

If you have any doubt as the validity of your P2PE solution and its eligibility for scope reduction and compliance assessment using the SAQ P2PE, you should engage with your vendor or solution provider to confirm all of those aspects discussed above as met. You may need to upgrade the solution, replace terminals, develop and implement policies and procedures to make sure that you have a P2PE Solution.

"Sysnet builds and supports mutually beneficial relationships between our clients and their customers globally through market-leading software, end-to-end services and best-in-class support."

Email: info@sysnetgs.com
Phone: +353 1 495 1300 | +1 404 991 3110
Web: sysnetgs.com

sysnet global solutions