Point-to-point encryption – an industry update

Mark McMurtrie, director of Payments Consultancy, analyses the impact of point-to-point encryption technology on the retail industry.
Published: 10:00:00 on the 15th Oct 2013Author: Ben Sillitoe

Compliance with the Payment Card Industry Data Security Standard (PCI DSS) has been a big headache for retail merchants over the last few years. But the importance of protecting customer details is well understood and accepted. However, greater priority needs to be given following the increasing attention of criminals and the large number of data breaches that are occurring. PCI DSS compliance has widespread implications for retailers as it incorporates: products, processes and people. It is not just an IT project but applies to the whole organisation and is an ongoing rather than a one-off task.

Retail stores are typically one of the most significant elements of a PCI DSS compliance project. This is largely due to the number of locations, systems, networks and hardware devices involved. It quickly becomes a scale game. The more stores, the larger the scope and higher the cost!
Retailers have constantly been on the lookout for ways to reduce the cost, timescales and scope of PCI DSS compliance. One new technology that is attracting lots of attention is point-to-point encryption (P2PE) this appears to offer many advantages. The way this works is to encrypt the card details as soon as the card is inserted into the card reader. By doing so, no card details are held or stored in the clear anywhere within the retailers systems. If there are no card details then there is nothing for the criminals to steal. The encryption need to take place within a secure element located inside the PIN pad. In order to be considered secure this PIN Pad must have been certified to the latest PCI PIN Transaction Security (PCI PTS) device standards and include a SRED secure element. *(Sorry for all the acronyms!)*
Unfortunately many PIN pads currently in use today do not meet these requirements and therefore a retailer would need to replace their devices with the latest models that do have the necessary certificates. Retailers will have to weigh up the benefits of scope reduction available from P2PE against the cost of early replacement of their PIN pad estate. Some may decide to wait until their next IT refresh before implementing P2PE.
The far end (point) of the secure channel is an application sitting within a data centre. It is here that the decryption takes place. This will be performed by a specialised payment application and a hardware security module (HSM). Early P2PE implementations had the retailer as the end point, but more recently we are seeing this extended to certain acquirers. It is also worth noting that Visa Inc has announced plans that they will be extending this even further by offering P2PE at a network level.
The two leading international PIN pad manufacturers both offer their own P2PE solutions. Ingenico call theirs On Guard and VeriFone's is marketed as VeriShield Protect. They offer these as managed service offerings or make their technology available directly to merchants, acquirers and payment service providers (PSPs). Additionally, several PSPs and payment application providers have been busy building their own P2PE solutions and trying to get them certified. These incorporate PTS SRED certified PIN pads. They have often needed to undertake further development in order to fully satisfy the assessors and payment networks. In order to fully comply with the P2PE standards encryption keys have to be loaded securely before usage (often at time of manufacturing) and also secure key management processes have to be put in place in order to update and manage encryption keys throughout their full lifecycle.
Merchants must take a close look at the PCI SSC website **www.pcisecuritystandards.org** where they can find a list of P2P Validated Applications. Currently there are only two listed and one of these is for a MPOS system designed for micro merchants. Also it is worth noting that as of today's date it appears that there are NO fully approved P2PE certified solutions despite what vendor literature may claim. Hopefully soon we will see greater availability of fully certified solutions. From what I hear it should not be too long a wait now.
All of this focus on P2PE is a good thing as it will strengthen the levels of data security protection and reduce the opportunities for fraudsters to steal card numbers.
P2PE offers the potential to reduce PCI compliance scope and even remove the EPoS store systems completely. This is not though guaranteed. There are caveats and so it is important that a retailer explains their plans to their security assessor and acquirer and hear what they think. They will then be able to provide the merchant with guidance. The devil is in the detail and you should be asking your potential vendor to see their P2PE certificate.