Update: The PCI SSC Releases its P2PE SAQ

In May the PCI Security Standards Council (SSC) published a fact sheet to offer guidance for merchants evaluating technology to accept payments using a smartphone or iPad/tablet. The fact sheet explains how a point-to-point encryption (P2PE) solution can be leveraged to secure mobile payments.

As a next step in its P2PE program, the SSC has released a P2PE Self-Assessment Questionnaire (SAQ). The new, reduced SAQ (SAQ P2PE-HW) is similar to SAQ B and contains 18 questions.

The PCI SSC website does not currently list validated P2PE solutions; however, the SSC plans to release the necessary documents for reporting and validation "in the coming weeks." Once this occurs, P2PE assessors, solution providers and application vendors can complete their assessments and submit their reports and validation documentation for acceptance and listing.

As the P2PE validation process progresses, merchants meeting the following criteria should use the SAQ P2PE-HW:

- Merchants processing cardholder data via hardware terminals included in a validated and PCI SSC-listed P2PE solution;
- Merchants who do not have access to clear-text account data on any computer system, and only enter account data via hardware payment terminals from a PCI SSC-approved P2PE solution; and
- Merchants who are brick-and-mortar (card-present) and/or mail-order-telephone-order (card-not-present) merchants. For example, a MOTO merchant could be eligible for SAQ P2PE-HW if they receive cardholder data on paper or over a telephone, and directly key it into a P2PE validated hardware device. Note that SAQ P2PE-HW would never apply to ecommerce merchants.

The merchants cited above would validate compliance by completing SAQ P2PE-HW and the associated Attestation of Compliance (AoC), confirming that:

- Their business does 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 hardware payment terminal used as part of a validated PCI P2PE solution;
- Their business has confirmed that the implemented PCI P2PE solution is listed on the PCI SSC's List of Validated P2PE Solutions;
- Their business does not store any cardholder data in electronic format, including no legacy storage of cardholder data from prior payment devices or systems; and
- Their business has implemented all controls in the *P2PE Instruction Manual (PIM)* provided by the P2PE Solution Provider.