P2PE vs E2EE Explained

May 13, 2016 PCI Blog E2EE, Encryption, P2PE, P2PE Instruction Manual (PIM), PA P2PE, Payments Industry, PCI Blog, PCI DSS, Point to Point Encryption (P2PE), PTS, SRED 5

If understanding the PCI scope reduction benefits of enterprise security solutions wasn't confusing enough, many companies have doubled-down by spreading misinformation around point-to-point encryption versus end-to-end encryption, or P2PE vs E2EE. As an independent IT security and PCI blog, we decided to write this article in an effort to provide clarity to merchants who are often mislead by sales folks within the payments industry. To begin the discussion, it's important to first understand **PCI Validated P2PE**. From there, we will discuss the differences – both from a technical and liability perspective – of P2PE versus E2EE.

PCI Validated P2PE vs. P2PE

PCI Validated P2PE is a unique standard from the PCI Security Standards Council, which was released in 2012. This is where the confusion begins. **PCI Validated P2PE does not equate to a P2PE solution that is simply PCI DSS compliant**. PCI DSS and PCI Validated P2PE, or just PCI P2PE, are two entirely separate standards and few companies in the world, let alone North America, have met the PCI P2PE standard. This is an extremely important point, as many P2PE solution providers claim that their solution is "PCI Validated P2PE" because they are also PCI DSS compliant. Don't fall for this sales trick. To view a full list of PCI Validated P2PE solutions and validate a sales person's pitch, click here to visit the official PCI Council website on approved PCI P2PE solutions: **https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions**

In an effort to avoid the confusion in the marketplace around PCI scope reduction, the PCI Council created the PCI P2PE standard to simplify the buying effort on behalf of merchants by standardizing P2PE, and offering a standard level of scope reduction. When a merchant opts-in to a PCI P2PE they are provided a P2PE Instruction Manual by the solution provider that breaks down their implementation requirements. We have more detail on the PIM here, **Understanding the P2PE Instruction Manual (PIM)**, but assuming a merchant implements their respective PCI P2PE solution properly, they automatically opt-in to the SAQ P2PE (or relevant controls for Level 1 merchants). We have the full SAQ P2PE v.3.2 on our **documents page**, and a quick review will show that your entire POS, network and supporting infrastructure is 100% removed from PCI DSS scope when utilizing a PCI P2PE solution.

Once again, this level of scope reduction can only be achieved by falling under the SAQ P2PE, and the SAQ P2PE only applies to merchants who are utilizing one of the PCI Validated P2PE solution providers listed on the PCI SSC P2PE website.

For a full breakdown of PCI Validated Point-to-Point Encryption, check out **PCI Validated P2PE Explained**.

P2PE vs E2EE – The Technical Difference

Now that we have a better understanding of PCI Validated P2PE, let's dig a bit deeper with the concept of P2PE vs. E2EE. P2PE, of course, stands for Point-to-Point Encryption, while E2EE stands for End-to-End Encryption. Leaving the compliance aspects aside for a moment, let's discuss the technical differences between P2PE and E2EE. Both P2PE and E2EE solutions encrypt payment data at point-of-interaction with the payment type (Swipe/MSR, Dip/EMV, Tap/NFC). From there, the data will be transported to the solution provider which, depending on the type of solution, will occur in a non-integrated, semi-integrated or fully-integrated fashion (another post to come on the differences between each). This is where the technical difference generally comes into play.

The solution provider, which is almost always a **payment gateway or back-end processor**, will decrypt the data for processing. For payment gateways, the packet is decrypted, and then sent to the relevant processor for processing in an encrypted, clear-text fashion. That being said, the connection to back-end processor, such as First Data or Elavon, is usually over a direct circuit or through a SSL/TLS-encrypted tunnel. In other words, the tunnel is encrypted but the data itself is not. Processors, who are usually the organizations pushing an end-to-end encryption solution for their own sales purposes, are also usually the organizations who spread misinformation on the topic. See, processors claim that E2EE solutions are more secure than P2PE solutions because the data itself is encrypted all the way to the "last mile" of the transaction, compared to P2PE solutions (payment gateways) that decrypt the data at the gateway level and then send it over an encrypted tunnel. From a security perspective, you could make the argument that E2EE solutions are more secure based on the technical definition described above. That being said, there are many ways to implement a security solution, and the most secure and trusted solutions will be those that have been validated by a third party Quality Security Assessor and have been certified to the PCI P2PE standard. Further, the merchant is only responsible for protecting its own environment, not that of the payment gateway or processor. With that, it follows that there's no additional scope reduction benefit from implementing an E2EE solution over a P2PE solution, and any data loss following transmission to a gateway/processor would be the legal responsibility of that gateway/processor, not the merchant.

Congratulations for reading this entire explanation! Your reward is $15 off of your next order with DCCS! Call us to place your order and mention your discount!