Payment Card Industry (PCI)

Point-to-Point Encryption (P2PE)

Frequently Asked Questions (FAQs): Assessment Guidance for Non-Listed Encryption Solutions

June 2020

Point-to-Point Encryption (P2PE) technology makes data unreadable so it has no value to criminals even if stolen in a breach. Merchants can take advantage of this technology with a PCI P2PE Solution: a combination of secure devices, applications, and processes that encrypt payment card data from the point it is used at a point of interaction (POI) device until it reaches a secure point of decryption.

PCI P2PE Solutions are validated by a P2PE QSA as meeting the rigorous security requirements of the PCI P2PE Standard and are listed on the PCI Security Standards Council (PCI SSC) website. These solutions can greatly simplify merchant efforts to comply with the PCI Data Security Standard (PCI DSS), by reducing where and how PCI DSS requirements apply. Recognizing that many merchants are not yet using PCI-listed solutions, however, the Council has issued Assessment Guidance for Non-listed Encryption Solutions to assist with evaluations of non-listed account data encryption solutions and their impact on merchants' PCI DSS compliance.

Q1 Why has the Council published this guidance?

A *PCI P2PE Solutions are account data encryption solutions that have been validated as meeting the PCI P2PE Standard and are listed on the PCI SSC website. Only these solutions have been independently assessed by a P2PE QSA and validated per the PCI P2PE Standard and Program Guide to provide the strongest protection for payment card data and greatly simplify PCI Data Security Standard (PCI DSS) compliance efforts, by reducing where and how PCI DSS requirements apply. The Council is encouraged by the significant growth of the PCI P2PE program since its inception and the increasing number of PCI-listed P2PE Solutions, Components, and Applications. At the same time, there are encryption solutions currently being used by merchants that are not PCI-listed. The Council recognizes this creates a challenge for Qualified Security Assessors (QSAs) in how they complete PCI DSS assessments for these merchants and that guidance is needed. The aim of the guidance is to provide a consistent approach for evaluating non-listed encryption solutions in use by merchant customers, and to reinforce that only PCI P2PE Solutions are tested and validated against the PCI P2PE Standard to provide the strongest protection for card data and reduce PCI DSS compliance responsibilities.*

Q2 Is this guidance endorsing the use of non-PCI listed account data encryption solutions?

A *No. Contact your payment brands and/or acquirer regarding the use of a non-PCI listed account data encryption solution.*

Q3 How should the guidance be used?

A *Assessment Guidance for Non-listed Encryption Solutions is guidance only, not requirements. P2PE QSAs can use the guidance to evaluate solution providers' non-listed encryption solutions and document their suggested impact on PCI DSS controls for merchants that use these solutions. The aim of a non-listed encryption solution assessment is to identify the gaps between the non-PCI listed solution in use and the PCI P2PE Standard and to show how use of the non-PCI listed solution might impact a merchant's PCI DSS assessment. Please refer to the guidance for more detail about the role of the various stakeholders and assessors involved.*

Q4 What’s the difference between this guidance and the PCI P2PE Standard?

A *The PCI P2PE Standard provides security requirements that must be met by a vendor’s encryption solution and validated by a P2PE QSA in order for it to be listed on the PCI SSC website as a PCI P2PE Solution.*

Only PCI P2PE Solutions are independently assessed by a P2PE QSA and validated per the PCI P2PE Standard and Program Guide to ensure the strongest protection for payment card data and simplify PCI DSS efforts for merchants. Many solutions currently being used by merchants are not PCI-listed, however, which is where this guidance comes in. It is for evaluating solutions that do not meet the PCI P2PE Standard, but are being used by merchants anyway, so that all the parties involved in a merchant PCI DSS assessment understand how the use of a non-listed encryption solution impacts the merchant’s PCI DSS compliance responsibilities.

Q5 What is the purpose of the guidance regarding non-PCI listed encryption solution assessments?

A *The aim of a non-listed encryption solution assessment is to identify the gaps between the solution in use and the PCI P2PE Standard and to show how use of the non-PCI listed encryption solution impacts a merchant’s PCI DSS assessment. This is done by the P2PE QSA filling out the Non-listed Encryption Solution Assessment (NESA) Template as well a P2PE Report on Validation (P-ROV) provided by the PCI SSC for the solution provider. The populated documentation from a P2PE QSA can be used by the merchant’s QSA as input to the merchant’s PCI DSS assessment. The guidance outlines the type of information that should be included in a non-listed encryption solution assessment.*

Q6 How does this guidance apply to PCI-listed P2PE Solutions?

A *The guidance does not apply to PCI P2PE Solutions (including P2PE Components or P2PE Applications) that are listed on the PCI SSC website. Only PCI-listed P2PE Solutions (including P2PE Components or P2PE Applications) are independently assessed by a P2PE QSA and validated per the PCI P2PE Standard and Program Guide to ensure the strongest protection for payment card data and simplify PCI DSS efforts for merchants. The Council continues to encourage merchants and acquirers to use the PCI SSC listing in selecting a PCI P2PE Solution that meets their needs.*

Q7 What is the benefit of using PCI-listed P2PE Solutions versus non-PCI listed encryption solutions?

A *Only PCI-listed P2PE Solutions have undergone an in-depth examination by a P2PE QSA and been validated against the P2PE Standard and Program Guide to ensure the strongest protection for payment card data and to significantly simplify the PCI DSS validation effort for merchants by reducing where and how PCI DSS requirements apply. This does not stop with validation***.** *These solutions are managed and updated according to a robust PCI Council program. This provides assurance to merchants that ongoing security is in place, including full re-assessment of the solution every three years, and annual checks in the meantime. To understand how the use of PCI-listed P2PE Solutions versus non-listed encryption solutions affect your PCI DSS compliance validation efforts, please contact your acquirer and/or payment brands.*

Q8 Does the Council have a program associated with this guidance?

A *No. This document is only guidance – it is not part of the PCI P2PE Program, nor any other PCI SSC Program. The PCI SSC does not approve, list, or certify anything based on this guidance.*

Q9 Does the Council list solutions based on this guidance?

A *No. The Council lists encryption solutions that have undergone an in-depth examination by a P2PE QSA and has been validated against the PCI P2PE Standard and Program Guide. There are no PCI listings associated with this guidance.*

Q10: Is the NESA template required to perform assessments of non-listed encryption solutions?

A *No. The NESA template is provided to facilitate the assessment of non-listed encryption solutions based on the guidance. The template creates a consistent approach to documentation completed by a P2PE QSA that is provided to the solution provider of the non-listed encryption solution for the benefit of their merchant customers using the solution. Contact your payment brands and/or acquirer for further information regarding the use of NESA documentation.*