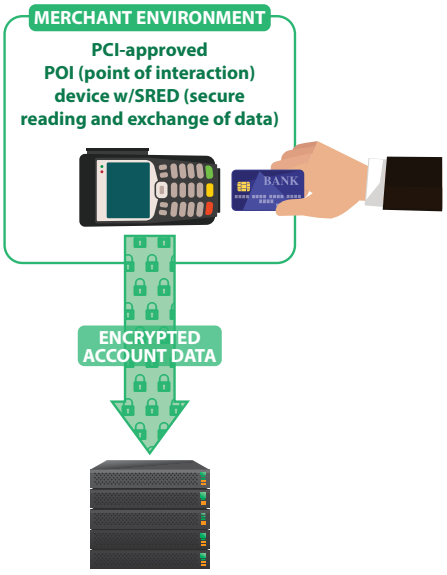
Securing Account Data with the PCI Point-to-Point Encryption Standard v3

A PCI-listed Point-to-Point Encryption (P2PE) Solution cryptographically protects account data from the point where a merchant accepts the payment card to the secure point of decryption. By using P2PE, account data (cardholder data and sensitive authentication data) is unreadable until it reaches the secure decryption environment, which makes it less valuable if the data is stolen in a breach. A PCI-listed P2PE Solution can significantly help to reduce the PCI DSS validation effort of a merchant's cardholder data environment. For more information and details about P2PE requirements, see the P2PE section in the Document Library on the Council's website. PCI P2PE version 3 simplifies the process for component and solution providers to validate their P2PE products for cardholder data protection efforts.



BENEFITS OF P2PE

- Makes account data unreadable by unauthorized parties
- "De-values" account data because it can't be abused – even if stolen
- Simplifies PCI DSS validation effort
- Offers a flexible solution for all stakeholders

More Flexibility for Solution Providers and Merchants

In response to the needs of P2PE community stakeholders, P2PE v3 brings more flexibility to solution providers – and in particular, to companies that provide components for integration within P2PE solutions. P2PE v3 is focused on modernizing, simplifying, and adding flexibility to the Standard, Program, and assessment process. This includes doubling the amount of component provider types that can get listed, which adds increased flexibility for Solution Providers. The listing of individual components makes it easier for a solution provider to be aware of and select validated components for integration. The same flexibility applies to merchants who are creating and managing their own P2PE solution.

Defining Elements of a P2PE Solution

P2PE Solution: A PCI-listed point-to-point encryption solution includes a combination of secure devices, applications and processes that encrypt cardholder data from a PCI-approved point-of-interaction (POI) device through to a secure decryption environment.

A P2PE Solution can also leverage the flexibility of using PCI-listed Components for integration into their Solution. Using a PCI-listed P2PE Solution minimizes exposure of clear-text account data within the merchant environment, rendering the data unreadable between the PCI-approved POI device and the secure decryption environment.

All PCI-approved solutions, applications, and components are listed on the Council's website. Validation is done by a PCI-qualified P2PE assessor.

July 2020

PCI Security Standards Council

Defining Elements of a P2PE Solution (continued)

P2PE Application: Software with access to clear-text account data, intended to be loaded onto a PCI- approved point of interaction (POI) device and used as part of a P2PE solution.

P2PE Component: A P2PE service that is accepted on a stand-alone basis as part of the P2PE Program and may be incorporated into and/or referenced as part of a P2PE solution.

A P2PE service is assessed to a specific set of P2PE requirements and results in a PCI P2PE component provider listing upon approval. P2PE component provider services are performed on behalf of other P2PE solution providers for use in P2PE solutions.

P2PE Solution Provider: An entity, usually a third-party such as a processor, acquirer (merchant bank), or payment gateway, that designs, implements, and manages the P2PE solution. The solution provider may outsource certain responsibilities, but will always retain overall responsibility for the P2PE solution.

Benefits of Using PCI-listed P2PE Solutions for Merchants

BETTER SECURITY

Protects your customers' data and your reputation.

PCI-listed P2PE Solutions provide the strongest encryption protection for your business. This means that your data is less valuable if stolen in a breach.

SIMPLIFY VALIDATION

Simplifies the PCI DSS validation effort.

PCI-listed P2PE solutions reduce the PCI DSS validation effort of a merchant's cardholder data environment.

MORE OPTIONS

Lets you do what you do best.

Now it's even easier to create and manage a solution yourself. Or, leave it to the solution provider to create and implement a solution that protects your customers' data and reduces your risk. Either way, you've got options to do what works best for your business.

Next Step?

Your organization's role in the payment system will determine the next step for P2PE:

- **Merchants:** Talk to your acquirer about selecting and using a PCI-listed P2PE v3 solution.
- **Merchant as a Solution Provider:** Talk to your acquirer and a qualified P2PE assessor about implementing and operating/managing your own P2PE solution.
- **Component Provider:** Talk to a qualified P2PE assessor about testing and qualifying your component for listing on the PCI Council's website.
- **Solution Provider:** Talk to a qualified P2PE assessor about testing and qualifying your solution for listing on the PCI Council's website.
- **QSAs / PA-QSAs:** Talk to the PCI Council about training and qualification to perform assessments of P2PE solutions, applications and components.

Use of P2PE v2 Solutions

Please note that the release of P2PE v3 does not impact the validity or merchant use of PCI-listed solutions assessed to P2PE v2.

July 2020

PCI Security Standards Council