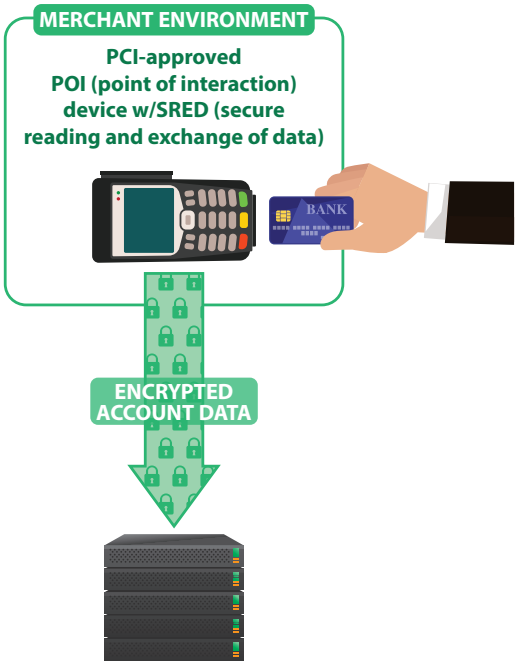
Securing Account Data with the PCI Point-to-Point Encryption Standard v2

A 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. Merchants using PCI-listed P2PE solutions also have fewer applicable PCI Data Security Standard (PCI DSS) requirements, which helps simplify compliance efforts. The PCI Security Standards Council has responded to market concern about the complexity of P2PE validation by updating the P2PE standard. Version 2 maintains this approach for protecting account data, while providing greater flexibility and more options for merchants and solution providers. For more information and details about P2PE requirements, see the P2PE tab in the Documents Library on the Council's website. This At a Glance provides highlights of P2PE v2.



BENEFITS OF P2PE

- Makes account data unreadable by unauthorized parties
- "De-values" account data because it can't be abused – even if stolen
- Simplifies compliance with PCI DSS
- The P2PE Self-Assessment Questionnaire includes only 26 PCI DSS requirements
- Offers a powerful, flexible solution for all stakeholders

More Flexibility for Solution Providers and Merchants

In response to the needs of P2PE community stakeholders, P2PE v2 brings more flexibility to solution providers – and in particular, to companies that provide components for integration within P2PE solutions. Previously, the PCI Council's website listed only validated P2PE solutions and P2PE applications; the listings will now include P2PE solution components, which are services that fulfill specific P2PE requirements. 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.

With P2PE v2, large merchants can implement and manage their own P2PE solutions for their locations – including implementation of requirements for separation between the merchant's encryption environment (their retail premises) and the merchant's secure decryption and key management environment. For details on this scenario, please see Domain 4 within the P2PE v2 standard.

June 2015

PCI Security Standards Council

Defining Elements of a P2PE Solution

A point-to-point encryption solution includes validated hardware, software, and solution provider environment and processes. It may also include validated services from a component provider. All PCI-approved solutions, applications, and components are listed on the Council's website. Validation is done by a PCI-qualified P2PE assessor.

P2PE Solution: Consists of point-to-point encryption and decryption environments, their configuration and design, and any P2PE components used with these environments. Within the P2PE solution, account data is always entered directly into a PCI-approved POI device with secure reading and exchange of data (SRED) enabled. This approach minimizes exposure of clear-text account data, and protects against point-of-sale exploits such as "memory scraping" malware.

P2PE Application: Software or other files 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 subset of P2PE services including encryption management, decryption management, and key injection, which are provided by a P2PE component provider and included in the P2PE component listing on the PCI website.

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. With P2PE v2, merchants may also chose to act as their own solution provider by implementing a merchant-managed solution (MMS).

Benefits of P2PE for Merchants

BETTER SECURITY

Protects your customers' data and your reputation.

Validated solutions provide the strongest encryption protection for your business. This means that your data is less valuable if stolen in a breach.

EASIER COMPLIANCE

Simplifies the PCI DSS compliance process.

PCI-listed P2PE solutions reduce where and how PCI DSS requirements apply to your business. This saves you time and money on overall compliance efforts without sacrificing the security of your customers' data.

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 v2 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.

About Use of P2PE v1.1 Solutions

Please note that the release of P2PE v2 does not impact the validity or merchant use of PCI-listed solutions assessed to P2PE v1.1.

June 2015

PCI Security Standards Council ®