



What is a point-to-point encryption (P2PE) solution?

According to the Payment Card Industry (PCI), a point-to-point encryption (P2PE) solution is a combination of secure devices, applications, and processes that encrypt data from the point of interaction (for example, at the point of swipe or dip) until the data reaches the solution provider's secure decryption environment. Provided by a third-party, a PCI-compliant SecureConnect must include all of the following:

- Secure encryption of payment card data at the point-of-interaction (POI).
- P2PE-validated application(s) at the point-of-interaction.
- Secure management of encryption and decryption devices.
- Management of the decryption environment and all decrypted account data.
- Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection, administration, and usage.

Why is P2PE so important?

With fraud on the rise, protecting sensitive cardholder data is more important than ever. According to Mastercard, the average cost of a card data breach in the retail industry is now a staggering $3.79 million, with average cost per stolen card reaching $165. Additionally, 70% of customers say they will avoid shopping at stores that have suffered a data breach. With a validated point-to-point encryption solution in place, any sensitive data intercepted between the merchant's card reader and the point of sale (or when being sent over the internet) will be useless to fraudsters, as it will have been encrypted and impossible to decipher. That gives merchants and their customers peace of mind in knowing that sensitive data is secure.





How does SecureConnect compare to our current EPX-Pay End-to-End Encrypted Solution (E2EE)?

End-to-end (E2EE) encryption refers to the entire transaction lifecycle being encrypted. Typically, hardware encryption is used at the point of interaction and the data stays in its encrypted state until it is received by the processor. Only then is the data decrypted and passed on to the card brands.

Our current EPXPay E2EE provides secure, end-to-end, PCI-compliant payment processing including EMV, tokenization, and encryption using our EPX international payment platform. However, E2EE alone cannot provide the full degree of PCI scope reduction available with PCI-validated P2PE. PCI P2PE-validated solutions like SecureConnect are vetted and independently audited by a 3rd-party QSA, confirming their adherence to the standard.

As an EPXPay integrated partner, what are the benefits of offering SecureConnect?

There are numerous benefits to offering SecureConnect to your merchants, including: it's the best security solution for card-present transactions, it saves them time and money, it protects their reputation, and it reduces their PCI scope.

SecureConnect adds value to your integrated solution by removing your entire POS, network, and supporting infrastructure from PCI DSS compliance requirements, leading to additional cost savings.

PCI-Authorized Scope Reduction is provided to merchants who use a validated solution like SecureConnect. Such merchants are eligible to complete the authorized self-assessment questionnaire SAQ P2PE that is known and accepted by all acquirers. Under PCI DSS v3.2, this means a significant reduction of controls, reducing the number of questions by nearly 90% for merchants moving from the SAQ D (329 questions) to SAQ P2PE (33 questions).





Does SecureConnect work with EPX BRIC tokens?

Yes, we will offer native support for the EPX BRIC token and EMV chip cards. Your current merchants will be able to keep their current EPX MIDs.

Which types of merchants should invest in a validated SecureConnect?

Any merchant who accepts card-present transactions can benefit from SecureConnect. Enhanced security, cost reduction, and brand protection are important for all card-present merchants, but especially for smaller, Level-4 merchants, which is where most data breaches occur.

EPX's validated SecureConnect is particularly suited to merchants in high-demand verticals such as higher education, healthcare, and government sector applications, where diverse card-present environments can be consolidated for PCI reporting purposes.

Can SecureConnect take POS data out of PCI scope?

About semi-integration: With the semi-integration solution approach, messages between the terminal and the merchant's POS system are limited to non-sensitive data and prevent card information from getting into the POS system. Instead, the card data is encrypted and routed directly from the terminal to the payment processor, completely away from the merchant's electronic cash register system, and back-office infrastructure. When you take the POS system out of the PCI equation, the semi-integrated solution reduces the compliance requirements and overall costs of adding an EMV-ready solution at a merchant's place of business.