securityMETRICS®

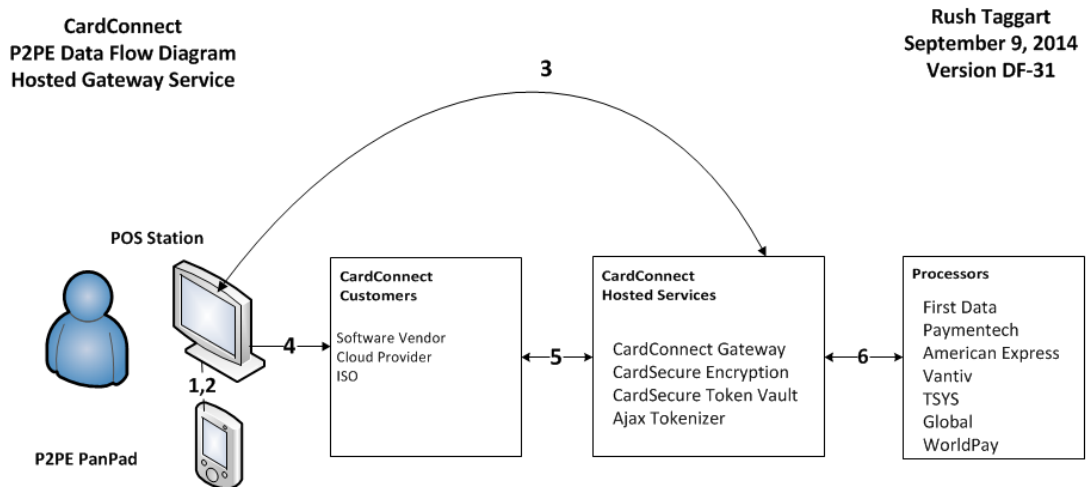
July 2, 2015

CardConnect
1000 Continental Drive, Suite 600
King of Prussia, Pennsylvania 19406

To Whom It May Concern:

As an authorized P2PE QSA company, SecurityMetrics conducted the P2PE solution assessment for the CardConnect Gateway service. This resulted in the "CardConnect P2PE" solution being listed on the Payment Card Industry Security Standards Council (PCISSC) web site as a fully P2PE validated. This letter is provided to clarify scoping questions for service provider customers of CardConnect who provide services or software to merchants (such as an Independent Sales Organization (ISO) or Independent Software Vendor (ISV)).

The diagram below illustrates the data flow of the payment data through ISO/ISV customers of CardConnect.



1) Payment card swiped or manually entered on CardConnect P2PE validated hardware terminal.
2) P2PE encrypted card data is obtained by CardConnect driver software installed on POS station.
3) P2PE encrypted card data sent directly to the CardConnect Gateway Service where it is decrypted and a token representing the card number is returned to the POS station.
4) Token (not card data) sent from the merchant POS station to the service provider (ISO, ISV, etc.) interface for payment processing. Note: token sent is neither card data nor P2PE card data.

5) Token is sent from the service provider to the CardConnect Gateway Service to continue payment processing.
6) Card data obtained after de-tokenization process in the CardConnect Gateway is sent to the desired processor or merchant bank for final payment processing. Success or failure is passed back to the POS station.

* The numbers above refer to annotations in the diagram.

As can be seen in the diagram and described above, the only place where P2PE encrypted card data travels is directly from the merchant POS station to the CardConnect Gateway service. The token returned from this process is not considered card data and therefore as it moves through a merchant system and then through another “in-line” service provider, like an ISV, the token does not cause any of those pathways to be brought into scope for PCI or P2PE security controls. Therefore, the in-line service provider has no PCI or P2PE scope if there are no payment card data pathways involved in their services other than those described above.

The merchant where the POS stations reside continue to have PCIDSS scope as the merchant is the signatory of the merchant agreement. The merchant must adhere to security requirements as required for the proper use of a validated P2PE solution (see PCIDSS SAQ P2PE-HW). Should the merchant have any credit card data processes in addition to or substantially different from the above, those must be scoped and the applicable security requirements implemented.

Service providers (ISO’s, ISV’s, etc.) working with CardConnect Gateway Services to deliver P2PE features to merchants in the manner described here have no need to validate to any PCIDSS or P2PE security requirements as they are not dealing with card data of any form.

SecurityMetrics is a privately held corporation based in Orem, Utah. SecurityMetrics is a registered PCI QSA, PA QSA, P2PE, ASV, and PFI Investigator with the PCI SSC. SecurityMetrics’ services and products include: vulnerability assessments, security appliances, on-site security assessments, forensic analysis, and penetration testing. Visa, MasterCard and American Express have certified SecurityMetrics programs for merchants who are required to adhere to the PCI Data Security Standard.

Regards,

Gary Glover
Sr. Director of Security Assessment, CISSP, CISA, QSA, PA-QSA
801-705-5638
gglover@securitymetrics.com