Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI Security Standards Council point-to-point encryption program update

August 29, 2011

In this statement the Council is updating stakeholders on the release of components of its program for validating point-to-point encryption solutions.

Point-to-point encryption technology may assist organizations to reduce the scope of their cardholder data environment and annual PCI DSS assessments. As implementation of these technologies grows, the Council believes it is imperative to build, test and deploy solutions that provide strong support for PCI DSS compliance. With this aim the Council will launch the first set of validation requirements for point-to-point encryption solutions. The Council reminds stakeholders that forthcoming requirements for validating point-to-point encryption solutions do not supersede the PCI Data Security Standard or other PCI Standards. The Council will provide security requirements, testing procedures, assessor training and resources to support the deployment of secure point-to-point solutions. However the launch of these requirements does not constitute a recommendation from the Council nor does it obligate merchants, service providers or financial institutions to purchase or deploy such solutions.

In September the Council will release validation requirements for hardware-based encryption and decryption solutions. Hardware solutions utilize secure cryptographic devices for both encryption and decryption including at the point of merchant acceptance for encryption and within Hardware Security Modules (HSMs) for decryption. Council will follow this with related testing procedures and then requirements for solutions that utilize software decryption within hardware, before the end of 2011. This second category of solutions combine hardware based encryption and decryption through a secure cryptographic device, with software that may manage transaction-level cryptographic keys for decryption.

In addition to these first steps focused principally on hardware, the Council will continue to explore the development of requirements for pure software solutions that encrypt cardholder data at the point of merchant acceptance, and/or decrypt cardholder data at a host system. Pure software solutions may use software to conduct encryption and decryption, performing cryptographic key management of both the master and transaction keys. Although industry standards bodies continue to require and/or strongly recommend hardware encryption and decryption, the Council will continue to work with key industry bodies to evaluate the feasibility of requirements for software-only based solutions.

As part of the first phase of the launch in September, the Council will be detailing the security requirements. Training to familiarize assessors with the program requirements and testing procedures is targeted for early 2012, with solution listings for hardware-based solutions following in the spring 2012. Further information will be shared with Participating Organizations and the assessment community before the North American Community Meeting, to prepare for discussions there.