Media Contacts

Laura K. Johnson, Ella Nevill
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org
Twitter @PCISSC

Payment Card Industry
Security Standards Council, LLC

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

PCI SECURITY STANDARDS COUNCIL PUBLISHES FIRST SET OF PCI POINT-TO-POINT ENCRYPTION SOLUTION REQUIREMENTS

- *New requirements focus on hardware-based solutions and support optional scope reduction efforts in a secure, PCI DSS compliant environment* -

WAKEFIELD, Mass., September 15, 2011 — The PCI Security Standards Council (PCI SSC), a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (PCI DSS), PIN Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS), today announced availability of the first set of validation requirements of its point-to-point encryption program. The PCI Point-to-Point Encryption Solution Requirements document provides requirements for vendors, assessors and merchants, that wish to build and implement hardware- based point-to-point encryption solutions that support PCI DSS compliance and offer scope reduction for merchants. Hardware-based P2PE 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.

The PCI Security Standards Council recognizes the potential for new technologies to reduce scope for PCI DSS assessments and provide new ways of securely handling cardholder data. This new document for vendors, assessors and solution providers that play a role in developing, implementing or assessing products, defines requirements for applicable point-to-point encryption (P2PE) solutions, with the goal of reducing the scope of the PCI DSS assessment for merchants using such solutions. Merchants themselves will also find the document a useful resource for understanding more about P2PE and PCI DSS scope. The new requirements do not supersede the PCI Data Security Standard, nor is a merchant mandated to use P2PE technology. However, merchants interested in this technology are encouraged to consult with the Council's

—more—

listing of validated P2PE solutions, targeted for spring 2012, to choose a secure solution that will support compliance with PCI Standards. The new requirements document includes information on:

- Roles and responsibilities in validating, implementing and assessing hardware based P2PE solutions
- Six critical domains of hardware-based P2PE that cover; the encryption device and environment, application security, transmission, decryption and key management.
- Steps required to create and validate a P2PE solution
- Visual representations of a typical implementation
- Interrelation between P2PE validation requirements and other PCI Standards such as PTS Point of Interaction (POI), PCI PIN, PA-DSS and PCI DSS

The hardware-based requirements incorporate many requirements and principles covering both physical and logical security that will be familiar to users of other PCI Standards. Requirements focus on securing systems and devices, implementing monitoring and response processes, developing and maintaining secure applications, protecting sensitive data, and using secure cryptographic key management methodologies.

“This is a solid first step in recognizing one popular type of deployment of P2PE solutions,” said Bob Russo, general manager, PCI Security Standards Council. “These P2PE requirements will help vendors, assessors, and merchants that are choosing to use hardware-based versions technology, to build, assess and implement P2PE solutions securely. If implemented in accordance with PCI requirements, P2PE solutions can significantly reduce a merchant’s card data environment, mitigate potential breaches and simplify PCI DSS validation efforts.”

Following the release of this first document the Council will introduce the associated testing procedures before the end of 2011. In addition, the Council will detail training opportunities for assessors and provide a listing of validated solutions on the PCI SSC website in spring 2012. As recently outlined in our program update, additional phases of the point-to-point encryption program this year will focus on requirements for solutions

that combine hardware based encryption and decryption through secure cryptographic devices, with software that may manage transaction-level cryptographic keys for decryption. The Council will also 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.

Click to Tweet: PCI SSC releases point-to-point encryption requirements for hardware-based solutions

About the PCI Security Standards Council

The PCI Security Standards Council is an open, global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and related standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., the Council has over 600 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: http://pcisecuritystandards.org.

Connect with the PCI Council on LinkedIn: http://www.linked-in.com/company/pci-security-standards-council
Join the conversation on Twitter: http://twitter.com/#!/PCISSC

###