Media Contacts

Laura K. Johnson
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 ANNOUNCES RELEASE OF NEWEST HARDWARE SECURITY MODULE (HSM) STANDARD

— Based on feedback from PCI community, updates to requirements enhance security of devices —

WAKEFIELD, Mass., May 31, 2012 —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 the introduction of the PCI PIN Transaction Security (PTS) Hardware Security Module (HSM) Security Requirements version 2.0, designed to secure cardholder data throughout the transaction process.

Hardware Security Modules (HSM) fall under the Council's PTS program and are non-cardholder facing devices used in connection with the protection of sensitive data, such as cardholder data and the cryptographic keys that protect or authenticate that information. For example, HSMs are used with PIN translation, payment card personalization, data protection and e-commerce.

The latest version of the HSM requirements is intended for HSM manufacturers to use in the development of their new products. The release of the new version of the PCI HSM requirements does not impact any payment card brand deployment mandate or current brand policy applicable to HSMs. As with other PCI device requirements, each individual brand determines the applicability of PCI approvals made against these requirements.

As part of a regular lifecycle for updating requirements, the Council has made a number of modifications to the existing security requirements to provide greater alignment

—more—

between the Hardware Security Module security requirements and the latest version of the PTS Point of Interaction (POI) Security Requirements.

Version 2.0 of the HSM Security Requirements provides additional physical and logical controls and processes to enhance the security of these devices. With these updates, vendors have more specific and robust criteria to build and test these devices against. Acquirers, processors and other HSM users are given a wider selection of HSM products to choose from, based upon their specific deployment needs.

The updates are based on input solicited from the PCI community during a formal feedback period earlier this year and include:

- The introduction of a two-tier approval structure that accounts for different deployments of HSM devices:
    - Controlled Environment – Approval is valid only when the device is deployed in a controlled environment as defined in ISO 13491-2 - which has more stringent access controls than the average computer room, with both its interior and the entrances under surveillance. The objective of a controlled environment is to limit the types of attack that can be made on a device.
    - Unrestricted – Approval is valid for any deployment
- Updated attack methodologies criteria to reflect more comprehensive threat assessment scoring
- Revised algorithms and key size requirements to be consistent with the latest version of the PTS POI Security Requirements and provide more secure data protection implementations as attack vectors advance
- Criteria to support remote key loading techniques using public key methods, as HSMs more commonly support networked (instead of only console) access to issue sensitive commands and to load cryptographic keying material
- Enhanced requirements for vendor-provided user security polices supporting the proper use and configuration of approved HSMs in a compliant manner, providing end users with more guidance for secure deployment

“HSM devices play an important role in securing certain critical data pieces in the card payment process,” said Jeremy King, European director, PCI Security Standards Council. “With the newest version of the HSM Security Requirements we have amplified the requirements to a higher security threshold and continued the evolution of the PTS standard, allowing vendors and users to produce and use more secure devices to protect their payment process.

The release of the updated requirements includes several supporting resources for PTS and HSM stakeholders:

- PCI PTS HSM Security Requirements 2.0 - contains the physical and logical security requirements as well as device management requirements and the forms to be used by laboratories and vendors
- PCI PTS HSM Security Requirements Modifications: Summary of Changes – provides explanation of key changes from version 1.0 to version 2.0 of HSM Security Requirements
- PCI PTS HSM Derived Test Requirements 2.0 - provides specific direction to vendors on methods the test laboratories may apply when testing against the requirements
- PCI PTS HSM Evaluation Vendor Questionnaire 2.0 - solicits additional information from vendors to support their claims of the conformity of their devices to those requirements.

After April 2013, all future HSM evaluations that result in a new approval must be conducted against version 2.0 of the PCI Hardware Security Modules Security Requirements version 2.0.

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 other 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: pcisecuritystandards.org.

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

###