Media Contact

Laura K. Johnson
PCI Security Standards Council
press@pcisecuritystandards.org
Twitter @PCISSC

Payment Card Industry
Security Standards Council, LLC

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

Payment Card Industry Security Standards Council Updates Hardware Security Module Standard

- Version 3.0 to Strengthen Security Requirements and Testing for Cryptographic Devices and Support Technology Solutions for Card Data Protection -

WAKEFIELD, Mass., 17 June 2016 — Today the PCI Security Standards Council (PCI SSC) published a new version of its device security standard for Hardware Security Modules (HSMs). HSMs are secure cryptographic devices that are used for cryptographic-key management and the protection of sensitive data used in payment card processing. HSM device manufacturers will use PCI PIN Transaction Security (PTS) Hardware Security Modular (HSM) Security Requirements Version 3.0 to ensure these devices provide the strongest protection for critical data elements used in card verification, PIN processing, chip transaction processing, payment card personalization, secure cryptographic key loading, remote HSM administration and other payment and authentication activities. Use of PTS validated HSM devices supports organizations in their efforts to secure payment card data throughout their systems and networks with PCI Standards.

HSM version 3.0 strengthens security requirements and testing for cryptographic devices and their use in supporting other technology solutions, including tokenization and point-to-point encryption (P2PE).

Key updates include:

- In support of PCI PIN Security and Point-to-Point Encryption requirements, a new approval class for key loading devices, which are devices that perform key injection of either clear-text or enciphered cryptographic keys or their components. The devices may perform other services such as key generation.
- In support of PCI Token Service Provider Requirements, a new approval class for HSM Remote Administration Platforms, which can be used for HSM configuration and key loading services without having direct physical access to the HSM.
- Significant enhancements of the test scripts for more robust validation against the existing security requirements, as well as the addition of numerous requirements and test procedures to support the addition of the two new approval classes.
- New testing requirements to ensure that PIN Transaction Security (PTS) evaluation laboratories will begin validating vendor documentation of vendor policies and procedures for compliance to the device management security requirements.

HSM version 3.0 is effectively immediately; however version 2.0 does not retire until 31 May, 2017 for new evaluations.

“Device security plays a critical part in protecting customer payment data before, during and after purchase,” said PCI Security Standards Council Chief Technology Officer Troy Leach. “We update PCI Standards to make sure that they continually provide the strongest protection for cardholder data. With HSM version 3.0, we’re doing that with more robust testing and validation, as well as new approval classes to provide enhanced support for PCI Standards and additional technologies for the protection of cardholder data. We encourage device vendors and Qualified Security Assessors (QSA) that deal with P2PE specifically to review and adopt the new HSM standard as soon as possible.”

A full copy of PCI PIN Transaction (PTS) Hardware Security Modular Security (HSM) Requirements Version 3.0 and supporting documentation including PCI PTS Hardware Security Module Summary of Requirements Changes from v2.0 to v3.0, PCI PTS Hardware Security Module Modular Derived Test Requirements, and PCI PTS Hardware Security Module Modular Evaluation Questionnaire are available at:
https://www.pcisecuritystandards.org/document_library.

About the PCI Security Standards Council

The PCI Security Standards Council is a 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. Connect with the PCI Council on LinkedIn. Join the conversation on Twitter @PCISSC. Subscribe to the PCI Perspectives Blog.

# # #