Payment Card Industry
Security Standards Council, LLC

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

Media Contacts

Laura K. Johnson
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org

PCI SECURITY STANDARDS COUNCIL RELEASES SUPPLEMENTAL GUIDANCE ON EMV AND POINT-TO-POINT ENCRYPTION

— Guidance provided to help the merchant community when considering point-to-point encryption and EMV implementations —

WAKEFIELD, Mass., October 5, 2010 — Today, 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), released guidance papers on the use of point-to-point encryption (P2PE) and EMV technologies in a payment card data environment.

Aimed at providing the market with greater clarity on how specific technologies relate to the PCI Security Standards and impact PCI DSS compliance, these papers are the first in a series of guidance documents the Council has committed to delivering as part of its ongoing assessment of emerging technologies.

Titled 'PCI DSS Applicability in an EMV Environment' and 'Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance,' the whitepapers are products of collaborative initiatives led by the Council's Technical Working Group (TWG) and Special Interest Groups (SIGs) in conjunction with the Council's constituents and industry experts including cryptographers, forensic investigators, standards bodies, PIN Transaction Security (PTS) labs, Qualified Security Assessors (QSAs) and vendors.

The guidance seeks to help the merchant community:

- Understand how these technologies help define or reshape the cardholder data environment
- Evaluate the impact of these technologies on PCI DSS compliance efforts
- Identify future potential for P2PE and EMV technologies

—more—

The Council's member organizations had the opportunity to review and discuss the papers at the PCI SSC North America Community Meeting in Orlando, Florida at the end of September.

"These documents were created as a direct response from our stakeholders and provide valuable background information for organizations that are considering implementations of EMV or P2PE technology within the context of PCI DSS compliance," said Troy Leach, chief standards architect, PCI SSC. "With this guidance we're helping them understand how they can better secure their payment card data and how specific technologies may assist them in meeting the requirements of the PCI DSS."

While EMV can substantially reduce fraud in card present transactions, the EMV guidance paper advises adopters that it does not automatically satisfy all PCI DSS requirements for the protection of cardholder and sensitive authentication data. In EMV environments, EMV technology and PCI DSS together provide the greatest level of security for cardholder data throughout the transaction process.

Currently no global standardization of point-to-point encryption technology or validation of its implementation exists in the industry. However by providing this new guidance on P2PE, the Council has taken the first step by definitively stating that P2PE may simplify PCI DSS compliance by reducing the scope of the cardholder data environment. In identifying the environments that still require the security protection of the PCI DSS, the guidance determines that P2PE solutions do not eliminate the need to maintain PCI DSS compliance for specific systems. It also recognizes the need for a set of criteria to validate the effectiveness of P2PE solutions so that merchants can have confidence that the solution they deploy properly secures cardholder data, which the Council plans to develop and release in 2011.

By outlining future considerations necessary to further address P2PE technology in the cardholder data environment, this document provides the industry's first roadmap for improving the security of payment card data and infrastructure as it relates to point-to-point encryption.

Both papers reinforce the effectiveness of the PCI DSS as a strong method for protecting cardholder data.

“It is important to remember that there is no silver bullet to securing a payment environment,” said Bob Russo, general manager, PCI SSC. “Implementing one of these technologies will not automatically make you compliant with the PCI DSS. Instead, organizations should focus on a layered approach to security. We believe the PCI Security Standards provide a solid foundation for a security strategy to look after your payment and other types of data, but security does not start and end with compliance. Focus on good security and compliance will follow.”

The documents, along with other Council educational resources, are available for download at https://www.pcisecuritystandards.org/education/info_sup.shtml.

The Council’s Special Interest Groups (SIGs) and other resources are actively engaged in the study of other technologies, such as tokenization, virtualization and bluetooth. In the future, specific papers and guidance from these groups will also be delivered and available on the Council’s website https://www.pcisecuritystandards.org/education/info_sup.shtml.

For More Information:

For more information on the PCI Security Standards Council, please visit www.pcisecuritystandards.org or contact the PCI SSC Secretariat for any questions or concerns regarding the Community Meetings at secretariat@pcisecuritystandards.org.

About the PCI Security Standards Council

The mission of the PCI Security Standards Council is to enhance payment account security by driving education and awareness of the PCI Data Security Standard and other standards that increase payment data security.

The PCI Security Standards Council was formed by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. to provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement and dissemination of the PCI Data Security Standard (DSS), PIN Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS). Merchants, banks, processors and other vendors are encouraged to join as participating organizations.

###