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 RELEASES PCI DSS TOKENIZATION GUIDELINES

—Merchants to benefit from guidance on how tokenization solutions may ease PCI DSS compliance efforts—

WAKEFIELD, Mass., August 12**,** 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 published the *PCI DSS Tokenization Guidelines Information Supplement*, the latest in a series of SSC guidance documents aimed at providing the market with greater clarity on how specific technologies relate to the PCI Security Standards and impact PCI DSS compliance.

Tokenization technology replaces a Primary Account Number (PAN) with a surrogate value called a “token.” Specific to PCI DSS, this involves substituting sensitive PAN values with non-sensitive token values, meaning a properly implemented tokenization solution can reduce or remove the need for a merchant to retain PAN in their environment once the initial transaction has been processed,

Working in conjunction with members of its Scoping Special Interest Group (SIG), the Council created the guidance in response to the requests from the PCI community for direction on how tokenization technology may reduce the scope of the cardholder data environment (CDE) and the effort required to conduct a PCI DSS assessment.

As with many evolving technologies, there is currently a lack of industry standards for implementing secure tokenization solutions in a payment environment. As part of an

—more—

ongoing evaluation of these technologies, this initial guidance from the Council provides stakeholders with suggested guidelines for developing, evaluating, or implementing a tokenization solution, including insights on how a tokenization solution may impact scope of PCI DSS compliance efforts.

Merchants are ultimately responsible for the proper implementation of any tokenization solution they use, including its deployment and operation, and validation of its tokenization environment as part of their annual PCI DSS compliance assessment. Organizations should carefully evaluate any solution before implementation to fully understand the potential impact to their CDE. The paper helps guide merchants through this process by:

- Outlining explicit scoping elements for consideration
- Providing recommendations on scope reduction, the tokenization process itself, deployment and operation factors
- Detailing best practices for selecting a tokenization solution
  Defining the domains, or areas that specific controls need to be applied and validated, where tokenization could potentially minimize the card data environment

This additional guidance also benefits tokenization service providers and assessors by informing them on how the technology can help their merchant customers limit or eliminate system components that process, store, or transmit cardholder data, and reduce the scope of the CDE – and thus the scope of a PCI DSS assessment.

“We’ve continued the process to investigate these technologies and ways that the community can use them to potentially increase the security of their PCI DSS efforts,” said Bob Russo, general manager of the PCI Security Standards Council. “These specific guidelines provide a starting point for merchants when considering tokenization implementations. The Council will continue to evaluate tokenization and other technologies to determine the need for further guidance and/or requirements. ”

Recommendations on the use of these technologies in relation to the PCI Standards are issued as separate guidance on an ongoing basis throughout the standards lifecycle.

The papers do not introduce additional requirements to the PCI Standards, nor are they an endorsement of one technology over another.

This newest guidance may be found in the Council's Document Library, an important collection of research, guidance and supplemental insight into topics that can aid ongoing PCI security programs.

"While this guidance will provide merchants with additional understanding on how tokenization may help their PCI efforts, it is important to note that tokenization should not be viewed as an alternative to the PCI Data Security Standard," said Russo. "Tokenization, implemented together with the PCI Standards, provides a layered approach to cardholder data security."

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 more than 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.linkedin.com/company/pci-security-standards-council
Join the conversation on Twitter: http://twitter.com/#!/PCISSC

###