Payment Card Industry
Security Standards Council, LLC

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

PCI SECURITY STANDARDS COUNCIL UPDATES PIN SECURITY STANDARD

—PCI PIN Security Standard Version 3.0 Incorporates ASC X9 TR-39 PIN Standard to Provide Unified PIN Security Standard for Payment Card Industry; PIN Assessor Program To Follow—

WAKEFIELD, Mass., 1 August 2018 — Today the PCI Security Standards Council (PCI SSC) published PCI PIN Security Requirements and Testing Procedures version 3.0, the PCI Security Standard for the secure management, processing and transmission of PIN data at ATMs and attended and unattended point-of-sale (POS) terminals. PCI SSC is also developing a program to train and qualify security assessors to support implementation of the PCI PIN Security Standard, to be available in 2019.

The updated PIN Security Standard is a result of collaboration between PCI SSC and the Accredited Standards Committee (ASC X9) to create one unified PIN Security Standard for payment stakeholders. It incorporates industry feedback received during a dedicated request for comments (RFC) period in 2017.

A summary of changes to the standard is available here. These include:

- The usage of personal computers for key loading, where clear-text secret and/or private keys and/or their components exist in unprotected memory outside the secure boundary of a secure cryptographic device (SCD), is being phased out at future dates.
- The allowance for the injection of clear-text secret or private keying material into an SCD is being phased out at future dates. Only encrypted key injection shall be allowed.
- Fixed key TDES PIN encryption will be disallowed at a future date.
- Host support for AES PIN encryption will be required at future dates.
- The test procedures have been enhanced to ensure more robust testing of existing requirements.
- The requirement that encrypted symmetric keys must be managed in structures called key blocks has been revised and broken into three separate phases, with different implementation dates, as outlined in the March 2017 PCI SSC bulletin on revisions to the implementation date for PCI PIN Security Requirement 18-3.

“For decades the use of verification methods, such as PIN, have provided additional authentication to protect payments from fraudulent use,” said PCI SSC Chief Technology Officer Troy Leach. “Version 3.0 of the PCI PIN Security Standard will ensure the continued integrity of PIN by minimizing future risk to key generation and operations. ASC X9’s contributions have been critical to this effort, and we look forward to our continued collaboration.”

“Version 3.0 of the PCI PIN Security Standard is a response to the payment card industry’s request for one unified PIN security standard,” said ASC X9 Executive Director Steve Stevens. “We are pleased to be working with PCI SSC on the integration of X9 TR39 and the PCI PIN Security Requirements into one standard that will simplify the security assessment process for stakeholders.”

Acquirers and their agents (e.g., payment processors, key-injection facilities, certificate processors, etc.) responsible for personal identification number (PIN) security and transaction processing should contact the applicable payment brands to understand the applicability of the revised standard to compliance validation requirements.

Organizations that previously used X9 TR-39 should check with the entity that required its use to confirm acceptability of using PCI PIN Security Requirements version 3.0.

PCI PIN Security Requirements version 3.0 and supporting documentation including the PCI PIN Security Requirements - PCI SSC Modifications – Summary of Significant Changes from v2.0 to v3.0 are available in the Document Library on the PCI SSC website.

PIN Assessor Program
A new PCI PIN Assessor program is in development for 2019, which will include the creation of the Qualified PIN Assessor (QPA) designation and a listing of Qualified PIN Assessor Companies in a manner similar to the existing Qualified Security Assessor (QSA) program. The use of QPAs will be determined by payment brand compliance programs. PCI SSC will keep stakeholders informed on the development and availability of the PCI PIN Assessor program.

About the PCI Security Standards Council
The PCI Security Standards Council (PCI SSC) leads a global, cross-industry effort to increase payment security by providing industry-driven, flexible and effective data security standards and programs that help businesses detect, mitigate and prevent cyberattacks and breaches. Connect with the PCI SSC on LinkedIn. Join the conversation on Twitter @PCISSC. Subscribe to the PCI Perspectives Blog.

About the Accredited Standards Committee X9 Inc.
The Accredited Standards Committee X9 Inc. is a non-profit organization accredited by the American National Standards Institute (ANSI) to develop both domestic and international standards for the financial services industry. X9 has over 100 member companies and over 400 company representatives that work to develop and maintain approximately 100 domestic standards and 58 international standards.
The subjects of X9's standards include: retail and mobile payments; printing and processing of checks; corporate treasury functions; block chain technology; processing of legal orders issued to financial institutions; tracking of financial transactions and instruments; tokenization of data; protection of financial data at rest and in motion; electronic contracts; and remittance data in business payments. X9 also performs the secretariat function and provides the committee chair for ISO TC 68, which produces international standards for the global financial services industry. For more information about X9 and its work, visit www.x9.org. Follow ASC X9 on Facebook, LinkedIn and Twitter.

Judith Vanderkay
ASC X9 Public Relations
1 (781) 883-3793
jvanderkay@gmail.com

Mark Meissner
PCI SSC Public Relations
1 (202) 744-8557
mmeissner@pcisecuritystandards.org

###