PCI PIN Security Requirements Updated

The Payment Card Industry Security Standards Council (PCI SSC), which manages security standards for the payment card industry, has published version 3.0 of the PCI PIN security requirements. This version recognizes Accredited Standards Committee (ASC X9) Technical Requirement (TR)-39 PIN requirements, thereby creating one industry standard for PIN data protection.

PCI PIN Security Requirements Updates

The PCI PIN security requirements define technical and procedural controls to assist with the secure management, processing and transmission of PIN data during online and offline payment card transaction processing at ATMs and POS terminals. The PCI SSC and the ASC X9 worked in collaboration to produce PCI PIN security requirements version 3.0, which incorporates TR-39 into the existing PCI PIN security requirements to create a unified PCI PIN security standard for all payment stakeholders.

All payment stakeholders are encouraged to review the *PCI SSC Modifications—Summary of Significant Changes from v2.0 to v3.0*, available online from the PCI SSC Document Library, for full details of the changes. In summary, PCI PIN version 3.0 changes 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), will be phased out.
- The allowance for the injection of clear-text secret or private keying material into a SCD will be phased out. Only encrypted key injection will be allowed.
- Fixed key Triple Data Encryption Standard (3DES) PIN encryption will be disallowed at a future date.
- Host support for Advanced Encryption Standard (AES) PIN encryption and decryption will be required at a future date.
- 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. These updates are outlined in the PCI SSC bulletin dated 28 March 2017 and "Implementation Date Change for PCI PIN Security Key Bundling Requirement," published in the 4 May 2017 edition of the *Visa Business News* available on Visa Online.

PCI PIN Assessors

A new PCI PIN Assessor Program is in development for 2019, which will include the creation of a new Qualified PIN Assessor (QPA) designation and listing of approved QPAs on the PCI SSC website. When established, the new QPA program will replace Visa's Approved PIN Security Assessor Program. PCI SSC will develop training and a certification program to ensure QPAs are adequately trained on the new PCI PIN version 3.0. Details to support the new QPA program and transition of Visa Approved PIN Security Assessors to the PCI SSC will be made available at a later date.

Effective Dates for Implementation

PCI PIN Security Requirements and Testing Procedures version 3.0, dated August 2018, is published and available on the PCI SSC Document Library (filter by PTS). All organizations should become familiar with the revised standard and associated impacts to their environment. There are a number of requirements that are future-dated; therefore, understanding the requirement and planning to meet the requirement by the stated date is necessary.

PCI PIN Security Requirements version 2.0 will still be the accepted standard for Visa compliance assessments and there are currently no changes for Validating PIN Participants or to the Visa Security PIN Program. Validating PIN participants must continue to use a Visa Approved PIN Security Assessors for onsite assessments.

In early 2019, once the PCI QPA certification program is established and assessors are trained, Visa expects to communicate and provide additional information on the transition for Validating PIN Participants to using a PCI QPA as well as when assessments to PCI PIN Security Requirements version 3.0 are required.

Visit Visa PIN Security at visa.com for up-to-date information on the Visa PIN Security Program and general PIN news, or contact your regional Visa PIN risk representative.

Additional Resources

Documents & Publications

The following documents are available at the PCI SSC Documents Library (filter by PTS):

- *PIN Security Requirements and Testing Procedures, Version 2.0, December 2014*
- *PIN Security Requirements and Testing Procedures, Version 3.0, August 2018*
- *PCI SSC Modifications—Summary of Significant Changes from V2.0 to V3.0, August 2018*

Online Resources

Visit the Visa PIN Security page for additional information.

Note: For Visa Online resources, you will be prompted to log in.

For More Information

For information on PCI PIN Security Requirements, email the PCI SSC at pcipts@pcisecuritystandards.org.

For more information on the PIN Security Program, PIN participant status or validation deadlines, contact your regional Visa PIN risk representative:

- **AP, CEMEA:** PINSec@visa.com
- **Europe:** VisaEuropePIN@visa.com
- **LAC:** PINLAC@visa.com
- **North America:** PINNA@visa.com
- **Global:** PIN@visa.com