Payment Card Industry
Security Standards Council, LLC

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

PCI Security Standards Council Bulletin: Implementation Dates for Key Block Equivalence

17 December 2020

The PIN Security Requirements specify the use of key blocks for the transport and storage of symmetric keys, i.e., AES and TDES keys. Allowed formats for these key blocks are defined by the standards bodies, ANSI and ISO. In addition, proprietary (i.e., non-ANSI or ISO recognized) methods have been allowed if 'equivalent'. In September 2020, the PCI SSC defined specific criteria that proprietary methods must meet in order to be verified as equivalent, including evaluation by independent experts providing security proofs and using the same peer review methods in use by the cryptographic community for validation of the veracity of the expert's analysis.

Based on industry feedback, the PCI SSC is providing additional clarification to ensure entities who are acquiring PIN based transactions and are using proprietary key block methods provided by either PTS vendors or other third parties have assurance that the methods they have in use are appropriately equivalent. Specifically, entities providing proprietary methods shall have until 1 January 2023 to:

- Obtain independent expert review of their method(s) and
- Where necessary, make any necessary design changes and
- Undergo appropriate peer review and
- Where changes to their existing method(s) are necessary, work with their clients to implement any necessary changes to the proprietary methods in use.

For meeting the PIN Security Requirements, these methods, if appropriately validated, will be recognized as equivalent.

Until January 2023, Service Providers, where applicable, can continue to operate using existing proprietary methods that have not yet been validated under the defined process. Any newly developed proprietary methods must undergo the defined process prior to any implementations.

The individual Payment Card Brands manage compliance programs for PCI Security Standards. Organizations should contact them directly with any questions.