Payment Card Industry
Security Standards Council, LLC

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

PCI Security Standards Council bulletin on revisions to the implementation date for PCI PIN Security Requirement 18-3

28 March 2017

Based on industry feedback, the PCI SSC is revising the implementation date for PCI PIN Security Requirements v2 Requirement 18-3 that states:

Effective 1 January 2018, encrypted symmetric keys must be managed in structures called key blocks. The key usage must be cryptographically bound to the key using accepted methods.

Acceptable methods of implementing the integrity requirements include, but are not limited to:

- *A MAC computed over the concatenation of the clear-text attributes and the enciphered portion of the key block, which includes the key itself,*
- *A digital signature computed over that same data,*
- *An integrity check that is an implicit part of the key-encryption process such as that which is used in the AES key-wrap process specified in ANSI X9.102.*

The new implementation dates are broken into phases, allowing organizations to focus resources on associated risk in order to achieve compliance. The phased implementation dates are as follows:

- **Phase 1** – Implement Key Blocks for internal connections and key storage within Service Provider Environments – this would include all applications and databases connected to Hardware Security Modules (HSM). Effective date: **June 2019.**
- **Phase 2** – Implement Key Blocks for external connections to Associations and Networks. Estimated timeline for this phase is 24 months following phase 1, or **June 2021.**
- **Phase 3** – Implement Key Block to extend to all Merchant Hosts, point-of-sale (POS) devices and ATMs. Estimated timeline for this phase is 24 months following phase 2 or **June 2023**.

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