Payment Card Industry
Security Standards Council, LLC

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

PCI Security Standards Council Bulletin: Revisions to the Implementation Dates and Scope for PCI P2PE Security Requirement 32-9

1 December 2020

Based on industry feedback, the PCI SSC is revising the implementation dates and modifying the POI device applicability for PCI P2PE Security Requirement 32-9. These changes are effective immediately. A P2PE technical FAQ will convey the revised requirement until such time the P2PE Standard is updated. The P2PE v3 Technical FAQs can be found here. The implementation dates have been deferred three years and the applicability changed from POI v3 and higher devices to POI v5 and higher devices as follows:

The revised P2PE v3.0 requirement 32-9:

The KIF must implement a physically secure room for key injection where any secret or private keys or their components/shares appear in memory outside the secure boundary of an SCD during the process of loading/injecting keys into an SCD.

The secure room for key injection must include the following:

- ***Effective 01 January 2024,*** *the injection of clear-text secret or private keying material shall not be allowed for entities engaged in key injection on behalf of others. This applies to new deployments of* ***POI v5*** *and higher devices. Subsequent to that date, only encrypted key injection shall be allowed for* ***POI v5*** *and higher devices.*
- ***Effective 01 January 2026****, the same restriction applies to entities engaged in key injection of devices for which they are the processors.*

Note: This does not apply to key components entered into the keypad of a secure cryptographic device, such as a device approved against the PCI PTS POI Security Requirements. It does apply to all other methods of loading of clear-text keying material for ***POI v5*** *and higher devices.*

Organizations should contact the P2PE program manager at p2pe@pcisecuritystandards.org with any questions.