

Does TDEA meet the requirements of "strong cryptography" as defined in PCI DSS?

PCI SSC FAQ | Article 1570 | August 2023

At the end of 2023, NIST disallows the use of three-key TDEA for use in protecting security sensitive data within US Federal information systems. However, as per NIST SP800-57 part 1, TDEA using three keys can still provide an effective strength of 112 bits when applied using appropriate key management and modes of operation.

The definition of 'strong cryptography' was updated in PCI DSS v4.0 to reference the effective key size of the algorithm/key combination rather than any specific algorithms - specifically the effective key strength is a minimum of 112 bits, with a recommendation to use systems that provide 128 bits of effective strength. Additionally, "strong cryptography" requires the use of industry-tested and accepted algorithms and proper key-management practices.

For other PCI SSC standards, refer to the subject standard for whether and how use of three-key TDEA is allowed.

Source: <https://www.pcisecuritystandards.org/faqs/1570/>