

Does PCI DSS define which versions of TLS must be used?

PCI SSC FAQ | Article 1491 | January 2021

No. However, PCI DSS does not consider SSL or early TLS to be strong cryptography.

Transport Layer Security (TLS) is a protocol that encrypts traffic between two endpoints to provide privacy and reliability of transmitted data and is widely used for internet communications and online transactions. Current available versions of TLS include TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3. PCI DSS does not allow the use of SSL or early TLS as a security control, with one exception. For allowed uses of early TLS, see the PCI SSC Information Supplement, Use of SSL /Early TLS for POS POI Terminal Connections.

The term "early TLS" does not refer to a specific version(s) of the protocol, but rather it encompasses any version or implementation of TLS that is vulnerable to a known exploit. This categorization is intended to help entities identify and prioritize mitigation efforts for TLS implementations known to be inherently vulnerable. Entities should have processes to monitor threats as they continue to evolve and as new versions of the protocol are released to address those threats, and to keep the entity's cryptographic implementations up to date to prevent them becoming vulnerable to known exploits.

All cryptographic implementations, including TLS, must use and support modern cryptographic algorithms, secure configuration settings, and other features as needed to meet the intent of strong cryptography. This means that every TLS implementation, irrespective of the protocol version, must apply strong cryptography using an appropriate cipher suite to implement a secure key exchange algorithm, strong cryptography, and an appropriate message authentication for strong cryptography and security protocols.

Entities using TLS should review their implementations against industry references (such as the current version of NIST SP 800-52) for guidance on configuration options that meet the intent of strong cryptography. Note that, while industry guidelines such as NIST SP 800-52 may provide additional insight into specific configurations and implementations and provide the rationale for implementing particular controls, PCI DSS does not mandate the use of external standards or guidance in meeting strong cryptography. In addition to monitoring specific threats to cryptographic implementations, entities should monitor changes in industry best practices and standards, and where applicable, entities should apply modifications to minimum cryptographic standards used within their environments to ensure that sensitive information such as account data and authentication credentials remain secured.

It is expected that systems conducting negotiation of TLS protocols use the strongest cipher suites first, with subsequent negotiation to mutually supported cipher suites only if needed, but always within the bounds of the minimum standard of strong cryptography and security protocols.

For the definition of "strong cryptography" as used in PCI DSS, refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms available in PCI SSC's Document Library, under the PCI DSS drop-down menu.

Source: <https://www.pcisecuritystandards.org/faqs/1491/>