

How does PCI DSS apply to EMVCo Payment Tokens?

PCI SSC FAQ | Article 1326 | May 2015

Payment Tokens, as defined by EMVCo in the "EMVCo Payment Tokenisation Specification - Technical Framework", are provided to merchants and acquirers in lieu of the cardholder's PAN. They are routed through the payment networks in the same way as a PAN and allow transactions to occur without the merchant being exposed to the underlying PAN.

Payment Tokens must be used in conjunction with a dynamic token cryptogram and/or other sufficient domain controls that are enforced during a payment transaction (as defined by the EMVCo Payment Tokenisation Specification - Technical Framework) to adequately prevent fraud. It is also not feasible to recover the PAN value associated with the Payment Token through knowledge of only the Payment Token, multiple Payment Tokens, or other Payment Token to PAN combinations.

Applicability of PCI DSS to Payment Tokens is described below.

For entities designated by EMVCo as Token Service Providers:

PCI SSC has published Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens), which is intended for Token Service Providers (TSPs) as defined by EMVCo. Within the TSP's token data environment, PCI DSS and the Additional Security Requirements for TSPs apply for the protection of Payment Tokens and payment card data. For more information about TSP requirements and the token data environment, refer to the Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens) and accompanying FAQ.

For all other entities (including merchants and acquirers):

A Payment Token that is defined and used in accordance with the EMV Payment Tokenisation Specification and that exists outside of the Token Service Provider's token data environment is not considered Account Data and is therefore not in scope for PCI DSS.

PCI DSS still applies anywhere Account Data is stored, processed, or transmitted. If any system storing, processing, or transmitting Payment Tokens also stores, processes, or transmits Account Data (such as a PAN), or is connected to systems that store, process or transmit Account Data, those systems remain in scope for PCI DSS requirements.

Please note that while some EMV-compliant chip cards and mobile phones may use Payment Tokens for payment, the use of an EMV-capable terminal or the acceptance of mobile or EMV chip transactions is not an indication that Payment Tokens are necessarily in use. Payment Tokens may be used in multiple types of payment transactions, including from chip cards, mobile devices, and card-on-file services. For more information about Payment Tokens, refer to the EMVCo website — www.emvco.com (<http://www.emvco.com>).

