TLS 1.2 Final Announcement

Overview

Under evolving PCI requirements and collective best-practice recommendations, Verifone will exclusively use the TLS 1.2 protocol on Commander starting with base 52. (Please note that throughout the first quarter of 2020, four major web browsers are also ending support for TLS 1.1.) This means that all communications to/from the Commander will exclusively use the TLS 1.2 protocol starting **February 17, 2020**.

The following table lists all supported Algorithms and Ciphers. The minimum Diffie-Hellman key exchange size for all ciphers listed is 2048 bits.

You can download the announcement here.

Table 1 – Cipher Suite, Names, and Descriptions for TLS V1.2

Short Name	Description
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	128-bit AES encryption with SHA-256 message authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate.
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	128-bit AES in Galois Counter Mode encryption with 128-bit AEAD authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate.
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	256-bit AES encryption with SHA-256 message authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate.
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	256-bit AES in Galois Counter Mode encryption with 128-bit AEAD authentication and ephemeral Diffie-Hellman key exchange signed with an RSA certificate.
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	128-bit AES encryption with SHA-256 message authentication and ephemeral ECDH key exchange signed with an RSA certificate.
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	128-bit AES in Galois Counter Mode encryption with 128-bit AEAD message authentication and ephemeral ECDH key exchange signed with an RSA certificate.
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	256-bit AES encryption with SHA-386 message authentication and ephemeral ECDH key exchange signed with an RSA certificate.
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	256-bit AES in Galois Counter Mode encryption with 356-bit AEAD message authentication and ephemeral ECDH key exchange signed with an RSA certificate.