How is Track 1 data encrypted?

ARTICLE INFORMATION:

SUMMARY: Credit card track data is typically read directly from magnetic stripe readers. Track 1 data contains the card account number (PAN) together with the cardholder's name, the expiration date and various other discretionary data fields. This article describes the restrictions placed on the input value and the algorithm applied by the SecureData Payments solution in encrypting these data.

INFORMATION:

APPLIES TO:

SecureData Payments POS SDK 2.2.1 and earlier (IB-KEEP v1)

Note: POS SDK 2.3 and later add support for IB-KEEP v2 algorithms, which are not covered in this article

MORE INFORMATION:

The Track 1 data format was originally defined by the International Air Transport Association (IATA). It contains up to a maximum of 79 alphanumeric, 7-bit (including parity) characters. Three special framing/field characters are defined: A start sentinel (%), an end sentinel (?) and a field separator (^). Otherwise, Track 1 values are generally comprised of digits [0-9], uppercase characters [A-Z], plus a few other characters such as spaces, periods, and a surname separator (/). In total, 64 characters are defined in the input alphabet, of which 18 (in addition to the three framing/field characters identified above) are reserved as special. No specific minimum length is defined, although at least 21 bits of data must be provided to successfully encrypt a Track 1 value.

An error is returned by the POS API if an attempt is made to encrypt a Track 1 value that is too long, too short or contains any character other than those defined as part of the input set. Note that the presence of a lowercase letter in the input value will cause an encryption failure. The output character set, used to represent the encrypted value, consists of the Base64 character set, which includes all upper- and lowercase letters, digits, together with the plus sign (+) and forward slash

Input Char Set	!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXZY[\]^_
Output Char Set	(/):+/0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz

It is therefore guaranteed that the sentinel characters and field separator will never appear in an encrypted value.

Because the output character set is the same *size* as the input character set, it is guaranteed the length of the ciphertext is always exactly equal to that of the plaintext value being encrypted, even though the actual character sets being used are different.

For example, the result of encrypting Track 1 data might appear as follows:

Plaintext	%B3333333310000000000^840JOHNSON/GEORGE^1 1062 22?
Ciphertext	w9KpXMJ8yXKSxRR0YeyHrKOA5NnnVCX3zyiQRHwEsodMC62gd

The actual ciphertext generated for any input value will, of course, depend on the symmetric key randomly generated on the POS device, although within a single cryptographic period (until key rollover is performed), the same plaintext value will produce the same result.

The underlying encryption algorithm used for Track 1 data is generally EME* (Encrypt-Mix-Encrypt) although the use of a Luby-Rackoff Feistel Construction (LRFC) is possible for shorter values (those containing no more than about 30 characters).