Methodology

Mobile SDK

Overview

There are two parts to the Mobile SDK, the end-to-end encryption method and the swipe device library.

End-to-End Encryption

The end-to-end encryption library allows credit card data to be encrypted on a mobile device before sending it to the Merchant's back-end server. During the sale process, the Merchant's server can send the encrypted card data to the Payment Gateway, where it is decrypted and treated like a normal credit card. This gives the merchant more control of mobile transactions without having to increase compliance costs.

The merchant's encryption key is an RSA public key that is unique to them. This means that the encrypted credit card data will only be able to be used to make a transaction in that merchant's payment gateway account. Only the Payment Gateway has access to the private key that corresponds to this public key.

Card data is encrypted using AES encryption with a new randomly generated key for every card. This key is then encrypted with the public key along with the card data. This packet (the encrypted card and AES key) is unreadable to anybody without the private key which is only known to the Payment Gateway.

Note: The public key cannot be used to decrypt an encrypted card. Once encrypted, the card is unusable except by the Gateway when it processes the payment for the merchant. For this reason, there is no need to keep the public key a secret.

Swipe Device Library

This library supports the encrypted card readers supported by the payment gateway. This includes parsing the data and notifying you when a card reader is connected, disconnected, ready to receive a swipe, etc.