



Encryption & Tokenization

What Is It and How it Helps Protect Cardholder Data

What is encryption?

Encryption takes the original cardholder data and an associated key and performs a mathematical operation against that data, resulting in what is essentially gibberish. To retrieve the original data, the associated key is used to decrypt the gibberish and return it to the original cardholder data.

What is Tokenization?

Tokenization is data substitution. It replaces data with a substitute—the substitute is a token which has no value.

How encryption works

Encryption helps protect cardholder data while it is in transit from when the data is captured through its transmission to the payment processor. This step means the transaction is never transmitted in plain text in the frame relay, dial-up or Internet connection, where the potential exists for interception.

How tokenization works

Encrypted cardholder data is received, decrypted and sent for authorization by Merchant Services via a secure channel. Once authorized, the cardholder data is sent to a centralized and highly secure server called a vault, where it is stored securely by Merchant Services. Simultaneously, a random unique number is generated (or an existing token is retrieved) that represents the cardholder data. This token number is returned to the business owner's system for use in place of the cardholder data.

The business owner receives the transaction authorization, permanently deletes the encrypted card data and retains the token number in its place. The business owner can store the token for settlement, reconciliation, chargebacks and other business-related purposes.

The business owner holds the token value and not the actual cardholder data. When the actual cardholder data is needed at some later time, a secure cross-referenced table allows authorized lookup of the original value, using the token as the index.