TransArmor Solution - Improving Security on Every Transaction

Tuesday, December 10, 2013 2:49 PM

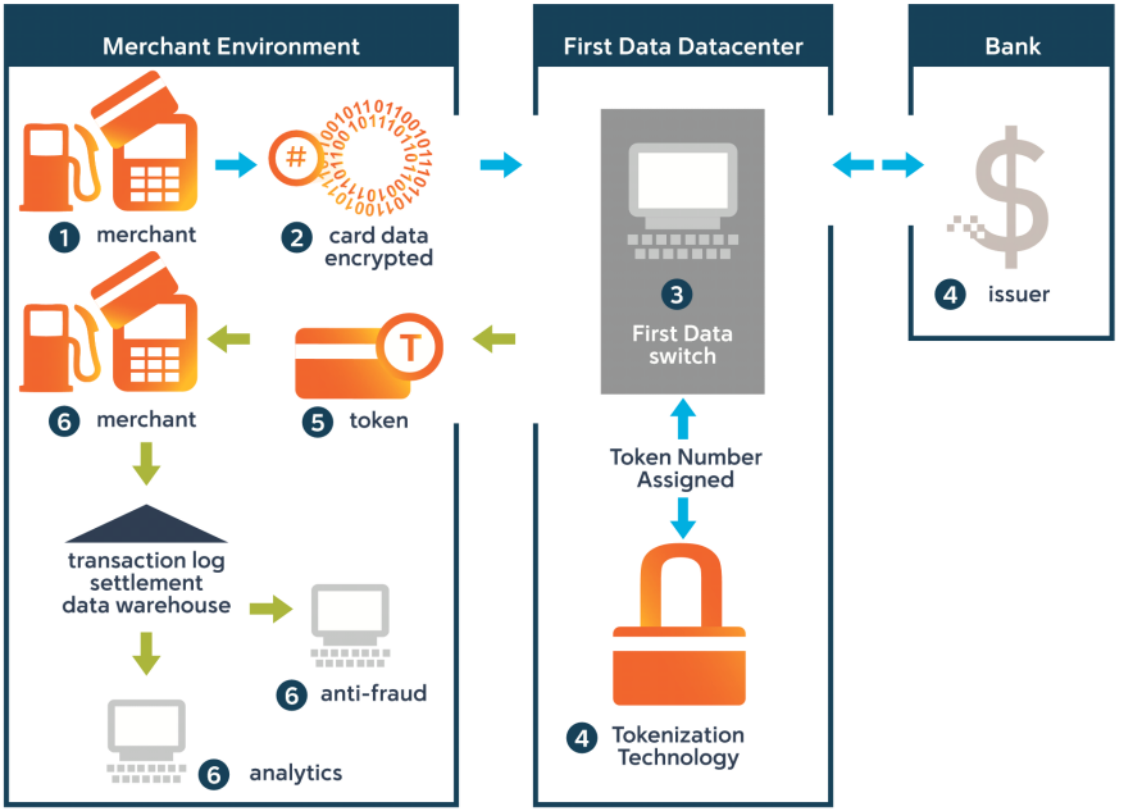
TransArmor® Solution

First Data™

Dual-Layered Payment Card Security

While encryption protects payment card data with an algorithm and a secret key, tokenization is the critical second security layer that completely eliminates card data from the environment, replacing it with a random-number token. Tokens are useless to criminals yet remain in the format of payment card data so merchants can carry out existing processes. Tokens also retain the business advantage of card data for analyzing customer buying behavior. This dual-layered security solution protects payment card data from the moment of initial capture through the entire payment process.

How the TransArmor Solution Works



1. Consumer presents card to merchant POS
2. Card data is encrypted and transmitted to First Data front-end
3. First Data front-end decrypts the data payload
4. Card data is sent to issuing bank for authorization and, in parallel, tokenized
5. Token is paired with authorization response and sent back to the merchant
6. Merchant stores token instead of card data in their environment and uses token for subsequent business processes

firstdata.com

TransArmor® Solution

First Data

Multi-Pay Tokens

The TransArmor solution includes the Multi-Pay Token option to support businesses that need to submit a financial transaction in a card-not-present situation. These tokens are unique to each merchant that uses them and are stored in place of the primary account number (PAN). With these tokens, merchants can initiate new or recurring payments within their own environment instead of using the original card number.

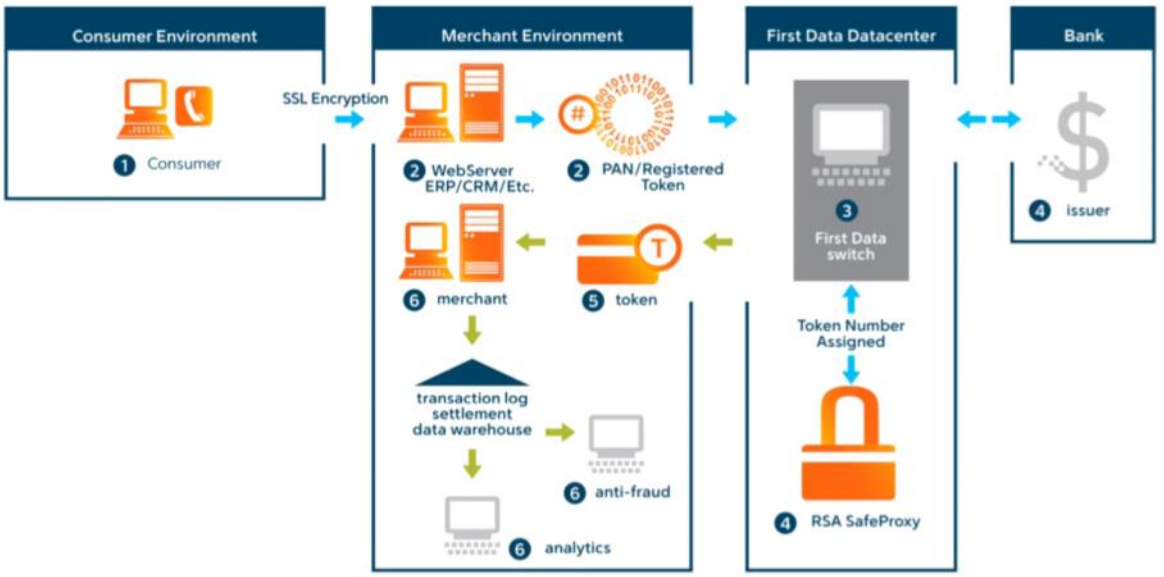
→ Valuable for eCommerce and card-not-present environments

→ Supports all businesses that rely on the ability to submit a sale transaction without card being present

→ Can be used for refunds and credits

→ Tokens let merchants track buying patterns for sales trending and marketing/loyalty programs while remaining PCI compliant

How TransArmor Works in a Card Not Present Environment



1. Card data is keyed into payment page/IVR. If e-Wallet technology is used, a consumer token can be used to initiate a new transaction
2. PAN is encrypted using session encryption and sent to First Data
3. Encrypted session is received at First Data datacenter
4. Card number is passed to bank for authorization and SafeProxy server for tokenization
5. Authorization and Multi-Pay Token are returned to the merchant
6. Multi-Pay Token is stored in place of the card number in all places
7. New financial transactions including sales, adjustments, refunds and settlement use the Multi-Pay Token instead of the PAN