

# Data Security Made Simple

Two Security Methods Combine to Secure Sensitive Cardholder Data

**Encryption** [en·krip·shuhn] – Algorithmic method that encodes plain text (such as a cardholder number) into a non-readable form called ciphertext

**Tokenization** [toh·kuhn·uh·zey·shuhn] – Method of replacing plain text (such as a cardholder number) with a randomized token number, or alias, that represents the actual plain text

**Encryption** works by taking the original cardholder data and an associated “key” and performing 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 plain text format. Generally, the keys and the encrypted data are kept within merchants’ data stores (i.e., onsite). The keys are the identifiers between the original data and the ciphertext and must be safeguarded, or the data protected by those keys could be compromised.

**Tokenization**, in its simplest form, is another way of saying “data substitution.” It is the act of replacing data that has value with a substitute—that substitute being a token number which has no inherent value. Thus, if the system using tokens is compromised, it is the token numbers that are taken, not the actual valuable data such as credit card numbers.

## How Encryption and Tokenization Work Together

Data is vulnerable at all points in card processing. No matter where cardholder data is during card processing, it is susceptible to security breaks. The three states of data—in transit, at rest and in use—cover the full spectrum of the life of sensitive data.

**In transit** – When data is moving from one device, application or system to another. This is where encryption fits into the combination solution for secure payment data transactions.

**At rest** (aka stored) – When data is stored somewhere for later use or for archival purposes. The benefits of tokenization start here.

**In use** – When cardholder data is used for business-related purposes other than for simply authorizing a payment transaction, such as analysis for marketing or loss-prevention. Tokenization continues to be the go-to technology of the combo solution.

Tokenization and encryption both specifically address the complex requirement to secure in-transit data and stored data. But tokenization also addresses the concerns of using sensitive data in business applications: the “in use” state of data.

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 by fraudsters.

With tokenization, encrypted cardholder data is received, decrypted and sent for authorization by the processor 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 the processor. Simultaneously, a randomly generated number, called a token, is generated (or an existing token is retrieved) that represents the cardholder data. This token number is returned to the merchant’s systems for use in place of the cardholder data.

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

The end result is that the merchant 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 held by the processor allows authorized lookup of the original value, using the token as the index.

## Card Fraud Fast Facts

“Consumers who are victimized react: 43% avoid the merchant, 31% spend less, 17% switch banks, 15% of issuers leave their banks” (2010 Javelin End-to-End Encryption, Tokenization ad EMV Analysis)

Existing card fraud increased 16% to reach \$22 billion in 2008 (2010 Javelin End-to-End Encryption, Tokenization ad EMV Analysis)

The average cost of coping with a data breach in 2009 rose to \$6.7 million (Ponemon Institute, 2009 Cost of a Data Breach Study)

## The Comprehensive Solution

To date there have been few easy and cost-effective solutions to the growing problem of managing the risks of handling sensitive payment card data. The consequences of a merchant data compromise in legal, financial, consumer confidence and brand loyalty terms can be enormous. (For more information on these specifics, see First Data's white papers: *Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance* and *PCI and Handling Sensitive Cardholder Data—Why You Care.*)

First Data, in collaboration with RSA—the security division of EMC, is launching a new service, the First Data® TransArmor<sup>SM</sup> solution, to help merchants of all sizes pro-actively address the vulnerabilities they face when capturing, processing and potentially storing consumer payment card data.

The TransArmor<sup>SM</sup> service provides an integrated solution to these challenges that will dramatically reduce merchant risk. TransArmor is an easy-to-implement service-based solution that protects merchants and consumers by encrypting vulnerable customer payment card data in transit, and, through tokenization, ultimately removing the need to store that data at the merchant level.

For more information about the new solution provided by the partnership of First Data and RSA, please contact your sales representative.

## Did You Know?

Small businesses are now being targeted by sophisticated and relentless criminals, who may be operating from down the street or half a world away. A Visa analysis found that small merchants accounted for more than 80 percent of the payment card data security breaches in 2007. So much for the idea that “it can't happen to me.”

There are numerous competitors active in the payments security space. Yet the category is still quite ambiguous to all audiences—including providers, merchants, and analysts. This is understandable: A wide variety of technologies are used; interpretations of terminology are varied; and a range of players from processors to individual technology providers are in the game.