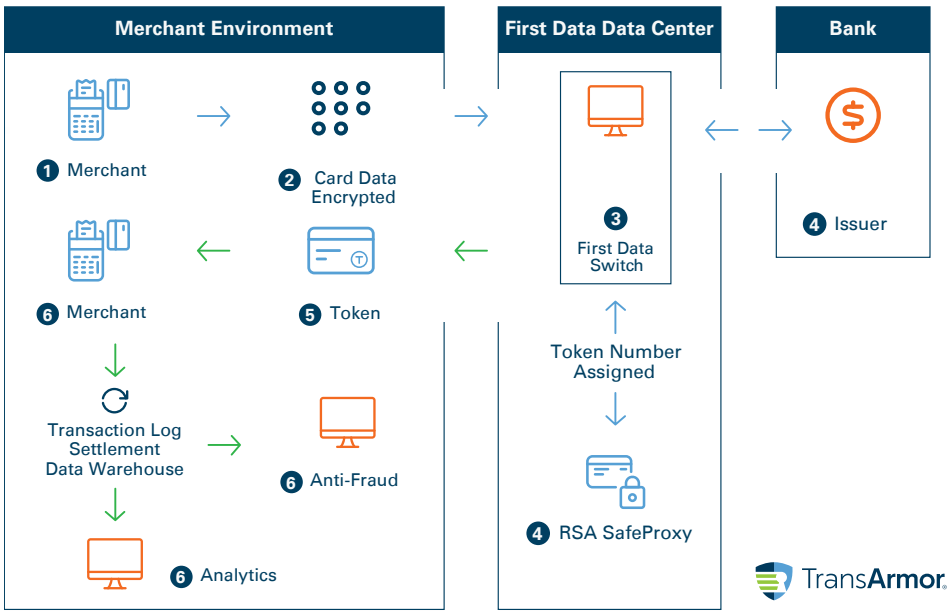
First Data is now fiserv.

First Data TransArmor FAQs

1. What is the TransArmor Solution?

TransArmor is a dual-layered payment card security solution that combines strong encryption and tokenization technology. TransArmor secures the transaction from the moment of swipe – prior to transmission and throughout the payment process with encryption, and it prevents card data from entering the merchant's card data environment (CDE) by replacing the primary account number (PAN) with a random-number token that can be safely stored.

2. How Does TransArmor Work in a Card-Present Environment?



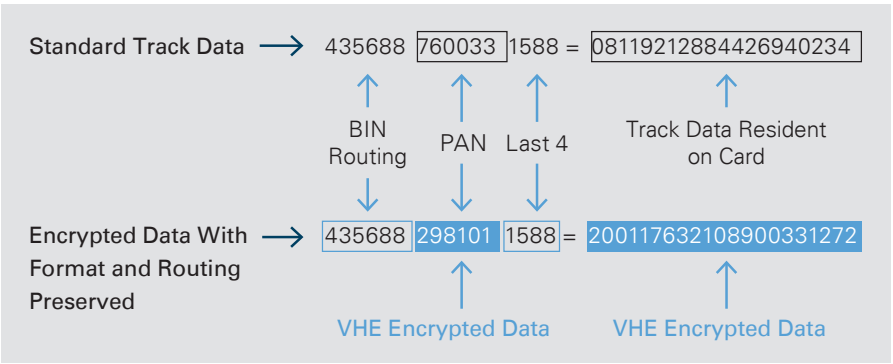
1. Consumer presents card to merchant
2. Card Data is encrypted and transmitted to First Data front-end
3. First Data front-end decrypts the data payload
4. Card data is sent to issuing bank for authorization and in parallel, tokenized
5. Token is paired with authorization response and sent back to the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

3. What Encryption Methods are Used in TransArmor?

There are four available encryption methods used in TransArmor: Three are Symmetric (shared key), and one is Asymmetric (public key).

TransArmor Verifone Edition (TAVE): Symmetric Key – Format Preserving Encryption (FPE)

- PAN and Discretionary data is encrypted at read in tamper-resistant hardware
- Supports mag-stripe, RFID, smart-card and manual entry
- Based on AES 128-bit algorithm
- FPE data resembles original target data



3DES: Symmetric Key – Non-Format Preserving Encryption (Non-FPE)

- 3DES is the common name for the Triple Data Encryption Standard algorithm (symmetric-key block cipher)
- 3DES applies the Data Encryption Standard (DES) cipher algorithm three times to each data block
- Supports mag-stripe, RFID, smart-card and manual entry
- 3DES keys must be loaded securely into the device either by First Data Hardware Services (fka TASQ), an approved ESO or through an approved Remote Key Injection method
- Non-FPE data does not resemble original target data

Track 2 Data –
5411110081111111=99122010
12340XXXX000

TDES Encryption Block –
F90209087AC4113D58B1AFB8C7248BCBE
010AF3B5B3CA10DDECAFF9EFBB6563598
60000A0ABB6F7B08534C06B5AXXXXX

Ingenico On-Guard: Symmetric Key – Format Preserving Encryption (FPE)

- Ingenico's proprietary Format Preserving Encryption is based on the 3DES algorithm
- PAN, Track 1 and Track 2 data is encrypted at swipe in an Ingenico device
- OnGuard 3DES keys must be loaded securely into the device either by First Data Hardware Services (fka TASQ) or Ingenico
- Supports mag-stripe, RFID, smart-card and manual entry
- FPE data resembles original target data

Unencrypted PAN – **5482650000007157**

Sample Encrypted Track 2 data:
548265111117157 = 34024860771111119749

Sample Encrypted PAN data (**PAN = ExpDate and CVV**)
M**5482651111117157** = 3402511

RSA/PKI: Asymmetric Key – Non-Format Preserving Encryption (Non-FPE)

- Uses the RSA 2048-bit algorithm
- Public Key resides on merchant device
- Private Key resides within First Data data center
- Supports mag-stripe, RFID, smart-card and manual entry
- Non-FPE data does not resemble original target data

PAN 4356887600331588 = qdjOJd1&22jIaowiAiwdj
(*882sSkw9IkwxMj2@j2
jjPxw8*nHg1#2134nnuw
NxdwKLwO

4. What is Tokenization?

- Tokenization is a form of data substitution
- TransArmor tokenization uses randomly generated numbers in place of PAN
- Tokenization differs from encryption: Tokens have no direct relationship with the data they replace
- TransArmor tokens are either universal or merchant-specific
- Tokens are card-based, meaning a merchant will always get the same token back for a specific PAN

Function	Merchant-Specific Token	Universal Token
One token per card/Shared merchants		X
One token per card/Per merchant	X	
Token can be used to initiate sale	X	
Token can be used for refund	X	
Token can be used for repeat/Recurring billings	X	
Last 4 of token match last 4 of card	X	X
First 12-digits are random	X	X
Token will fail mod10 check	X	X
Token can be used to adjust sale (if not settled)	X	X

5. As a Vendor, What Are the Benefits of Supporting TransArmor?

- Reduces the costs associated with PCI compliance in three ways:
  1. Shrinks the vendors card-data environment (CDE)
  2. Simplifies the questionnaire that the vendors customers must answer
  3. Changes the answers of some questions to N/A
- Removes the risk of storing card data, transferring it to the processor
- Allows the vendor to focus on projects that contribute to revenue rather than securing cardholder data

6. How Do I Support TransArmor?

Listed below are the First Data specifications that support TransArmor:

BuyPass® – ATL105, Host/Controller, ISO8583

CARDnet® – ISO 8583 with and without PTS Settlement, EDC

Nashville – ISO 8583 with and without PTS Settlement

Compass – Batch/Online

Omaha – ETC+

Front-end/Back-end combinations

	Front-end platforms				
Back-end Platforms	**Compass**	**North Nashville**	**North CARDnet**	**Omaha**	**BuyPass**
North	x	x	x		x
South		x			
Omaha				x	
Memphis					x

Not Supported X = Supported Future = Planned but no release date set

	Compass	North	Nashville	Omaha	BuyPass
Encryption and Tokenization		X	X	X	X
Tokenization Only	X	X	X	X	X

Note: For PIN pads and PIN pad software-related questions, we recommend contacting your sales support contact at the hardware manufacturer.

7. Will I Need to Certify/Re-certify for PA-DSS/PCI Compliance?

Contact your QSA for direction. Note that First Data does validate application name and version for PA-DSS/PCI compliance before releasing any product into production.

fiserv.com

First Data is now fiserv.