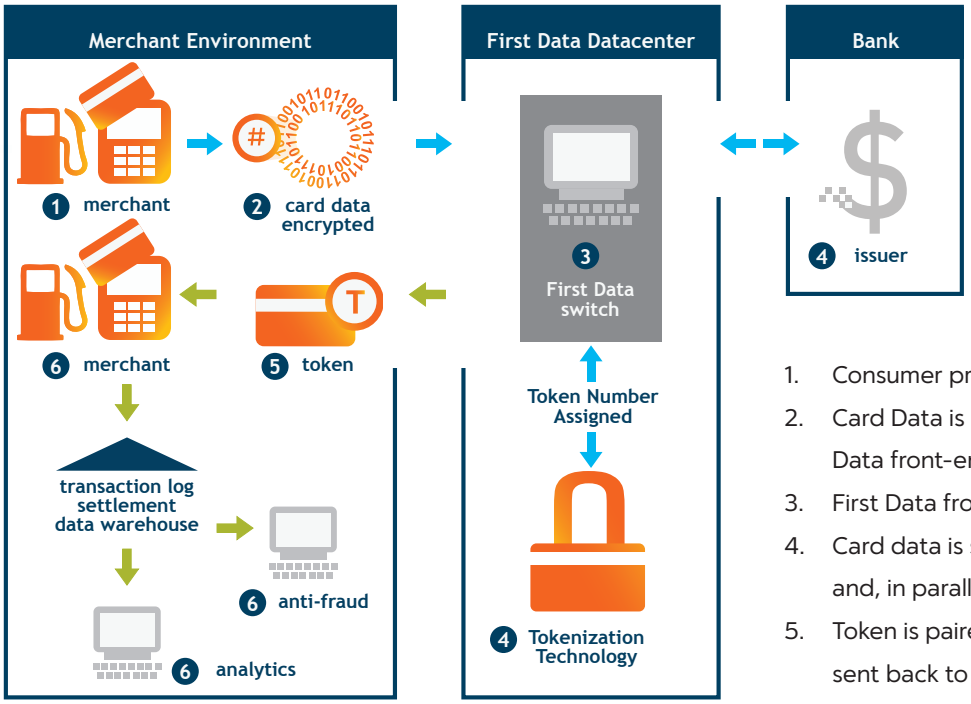
The First Data® TransArmor® FAQs

1. What is The TransArmor Solution?

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

2. How Does TransArmor Work?



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

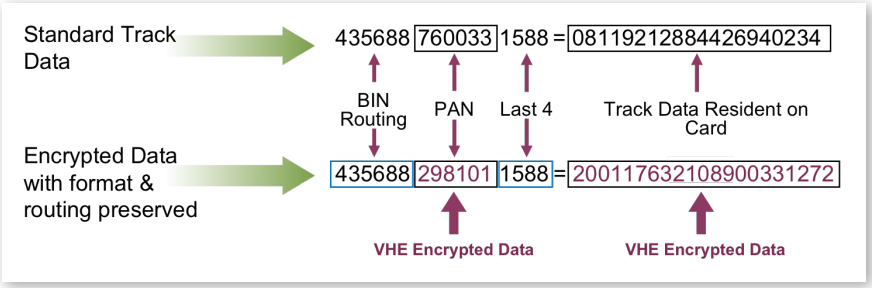
The First Data® TransArmor® FAQs

3. What encryption methods are used in TransArmor?

There are two types of encryption used in TransArmor: Symmetric (shared key) or Asymmetric (public key)

Symmetric Key: VeriShield

- PAN and Discretionary data is encrypted at read in tamper resistant hardware.
- Supports mag-stripe, RFID, and smart-card
- Uses 128-bit AES, format-preserving, symmetric-key encryption



Asymmetric key: RSA Encryption

- Uses the RSA 2048-bit algorithm in software
- Public key resides on merchant device
- Private key resides within First Data datacenter
- In the message spec, the STM encryption type is '001'
- We encrypt Track 1 and Track 2 data
- Encrypted data does not resemble original data and is not put in the PAN field, but is appended at the end of the message

4356 8876 0033 1588 =

qdjOJd1&22jlaowiAiwdj
(*882sSkw9IkwxMj2@j2jjPxw8*nHg1#213
4nnuwNxdwKLwO

4. What is Tokenization?

- Tokenization is a form of data substitution
- TransArmor tokenization uses randomly-generated numbers in place of primary account numbers (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 to 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

The First Data® TransArmor® FAQs

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		Future			
Omaha				x	
Memphis					x

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

	Compass	North	Nashville	Omaha	BuyPass
Encryption & Tokenization		X	X	X	X
Encryption Only					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.

b›yond the transaction℠