First Data®

BUYPASS® Platform
Host and Controller Interface Specification Updates for TransArmor® Processing

Version: 2023-1

August 18, 2023

Copyright

Disclaimer

The TransArmor Addendum should be used in conjunction with BUYPASS® Platform Host and Controller Interface Specifications.

Please subscribe to this TransArmor Addendum by checking the subscribe button on the First Data specification website prior to download, so notification will be emailed when new versions are available. Please send an email to certsupport@firstdata.com for additional information.

Revision History

This document replaces the following document:

- *BUYPASS® Platform Host and Controller Interface Specifications Updates for TransArmor Processing*

  Specification Release Date: June 26, 2020

  Specification Release Version: 2020-1

The following table lists added, updated, and deleted pages:

Note: Red text and change bars in the page margin indicate updated/added text. Deleted text is indicated only in the following table. Blue text indicates a link to another location in the text.

Changes Made to Ver. No. 2020-1 and Reflected in Ver. No. 2023-1 Released August 18, 2023			
Topic	**2020-1 P. No.**	**2023-1 P. No.**	**Summary of Change**
E2D Updates	NA	37	Added note on restarting the key exchange process under TransArmor® CA Key Exchange Process Flow
	NA	41	Added verbiage on restarting the key exchange process under Certificate Authority Key Rotation

Table of Contents

1. Introduction

This document provides information about the requirements for implementing TransArmor transaction processing interface between a customer's host system (host-to-host gateway) or a customer's device controller system (controller-to-host).

The primary audience of this document includes the merchant or vendor implementing TransArmor processing services.

1.1 Chapter Conventions

This document follows certain typographic conventions in text to help you identify special terms and notes. The following table describes these conventions and provides examples of their usage:

Chapter Conventions

Convention	Description	Example
Copyright Information	The copyright symbol for TransArmor is used only in the headings of the main chapters and the sub chapters.	What is TransArmor®? First Data provides an advanced mode of payment card security service through its TA solution.
TransArmor/TA	In headings and introduction of a section, TransArmor is written in full form, however, in the body of the content, the acronym "TA" is used.	First Data provides an advanced mode of payment card security service through its TransArmor (TA) solution. The TA solution is developed through partnership between First Data, VeriFone Systems, and RSA, the Security Division of EMC.
Subsequent/Follow-on Transactions	This is a collective noun phrase used to denote the transactions that are based on the original authorization request.	The list of subsequent transactions is given below: • Completion • Reversal • Void
Bulleted List	All instances of an unordered series of concepts, items or options are represented in the form of bullets.	Following are the benefits of TA: • Payment card security solution that removes sensitive payment card data from the merchant environment to reduce the threat and liability associated with a data breach • Dual-layered solution combining encryption + tokenization technology to fortify the merchant environment with an end-to-end solution that comprehensively protects payment card data

Chapter Conventions		
Convention	**Description**	**Example**
Numbered List	All instances of sequence of processes, events or steps are represented in the form of bullets.	1. The POS device sends a TA Signing Key and Signed Key ID Load message requesting for Signing Key 2. The POS device receives the Signing Key in the TA Signing Key and Signed Key ID Load response from First Data

1.2 List of Acronyms

In this document, all instances of terms, such as, TransArmor/ Data Encryption Key/ Certificate Authority/ Security Packet, etc, used as proper and common nouns in sentences in the chapter's body are represented through acronyms. The table below gives you the list of the acronyms, used across the document.

Acronyms	
Acronym	**Description**
TA	TransArmor
DEK	Data Encryption Key
DDK	Data Decryption Key
SP	Security Packet
CA	Certificate Authority
CA-ID	Certificate Authority Identifier
TA-VE	TransArmor –VeriFone Edition
TRSM	Tamper-Resistant Security Module
SRED	Secure-Reading and Exchange of Data
AES	Advanced Encryption Standard
VAR	Value Added Reseller

Note: Terms present in request/response formats and value sets are not represented through acronyms for better understanding.

This document contains the following chapters and appendices:

1. **Introduction.** This chapter describes the purpose, usage, target audience, chapter conventions and list of acronyms used in this document. It also provides a list and describes each chapter and appendices present in the document.
2. **Overview.** This chapter provides a general overview on TransArmor.
3. **TransArmor® Encryption and Tokenization.** This chapter describes the TransArmor encryption and tokenization methodologies and supported transactions.
4. **TransArmor® CA Certificate Overview.** This chapter describes the CA Certificate Overview and process flows.
5. **Impacted Data Elements.** This chapter describes the Data Elements which have been impacted by TransArmor transaction processing.

2. Overview

This chapter discusses the following TransArmor processing overview:

- What is TransArmor®?
- Why is TransArmor® Highly Recommended?
- TransArmor® Data Protection
- TransArmor® Security Solutions

2.1 What is TransArmor®?

First Data provides an advanced mode of payment card security service through its TransArmor (TA) solution. The TA solution is developed through partnership between First Data, VeriFone Systems, and RSA, the Security Division of EMC. Following are the benefits of TA:

- Payment card security solution that removes sensitive payment card data from the merchant environment to reduce the threat and liability associated with a data breach
- Dual-layered solution combining encryption + tokenization technology to fortify the merchant environment with an end-to-end solution that comprehensively protects payment card data
- The world's most widely used payment security product - safeguarding 400,000+ merchant outlets and 1 billion transactions+ since its launch in 2010
- Flexible solution that can be implemented on First Data or 3rd Party (VeriFone, Equinox, Ingenico, etc.) devices via hardware (VeriFone only) or software-based encryption and tokenization
- PCI DSS compliant solution - TransArmor exceeds PCI requirements
- Easily integrates with a variety of merchant payment applications via Rapid Connect, to let customers pay anyway and anywhere they choose

2.2 Why is TransArmor® Highly Recommended?

During a transaction processing, the cardholder data flows through multiple entities, technologies, and applications. This long chain of processing units increases high risk of data breach at every step of the transaction flow. Generally, the sensitive cardholder data is at risk of being exposed or stolen at the following two steps in the transaction flow:

- Pre-authorization - In this scenario, a merchant captures the customer’s data to send it to the acquirer/processor. Therefore, at this stage the data is either being sent or is waiting to be sent to the acquirer/processor.
- Post-authorization – In this scenario, the acquirer/processer has already sent back the authorization response to the merchant, and the response data is stored in the merchant environment to be used for analytics and other back-office processes.

2.3 TransArmor® Data Protection

TA security system protects the cardholder data at the following stages in processing:

- In transit: - The sensitive data is protected in transit with advanced encryption options that secure data from the moment of swipe throughout the transaction.
- In use: The sensitive data is removed from the card data environment (CDE) after authorization by replacing the sensitive data with a token or randomly generated number.
- At rest: The non-sensitive tokenized card data is stored safely for back-end business operations and customer analytics. Tokenization of card data reduces the risk of loss of data, minimizes brand damage, and builds customer confidence. TransArmor also reduces the security threat that could result in financial liability and litigation.

2.4 TransArmor® Security Solutions

TransArmor offers two Security Solutions:

- Encryption and Tokenization: This method supports the use of card data encryption and the use of Token. TA enabled terminals encrypt the cardholder data that is present in the initial transaction request. In subsequent transactions with the same card, the token received from First Data is used in place of a card's Primary Account Number (PAN).
- Tokenization Only: The POS device must send the PAN in the clear during initial the transaction to get back a token in the response. In subsequent transactions using the same card, the token received from First Data must be used in place of the card's PAN.

Additionally, there are two Encryption options to choose from and two Tokenization Types to choose from, outlined in the matrices in Chapter 3. TransArmor® Encryption and Tokenization.

3. TransArmor® Encryption and Tokenization

This chapter discusses the following:

- TransArmor® Encryption Methods
- TransArmor® Tokenization
- TransArmor® CA Certificate Overview

3.1 TransArmor® Encryption Methods

- RSA's Public Key Infrastructure (PKI) encryption provides software-based encryption. This method uses the RSA 2048-bit algorithm in software. PKI can be installed on terminals or PC-based POS devices, letting you add the TransArmor solution with little-to-no investment in new or upgraded hardware
- TransArmor - VeriFone Edition (TA-VE) encryption provides hardware-based, format-preserving encryption. This method uses 128-bit AES symmetric key encryption. TA-VE can be installed on standalone and integrated VeriFone devices. The installation of TA usually requires no software-related modification at the POS application level and no extra steps or training for the retailer

TransArmor Encryption Differentiators		
Method	**TransArmor Public Key Infrastructure (PKI)**	**TransArmor VeriFone Edition**
Technology Partner	RSA	VeriFone
Aliases	• Software-based encryption • RSA encryption • Asymmetric encryption	• Hardware-based encryption • Format-preserving • Symmetric encryption
Summary	Uses two separate keys to protect data: a 'public key' and a 'private key'. Public key is used in the merchant environment to encrypt the cardholder data and the Private key is stored in a Host Security Module (HSM) within First Data's secure environment and is used to decrypt the cardholder data.	Uses VeriFone's existing PCI PTS-approved payment devices, encryption is performed within a Tamper-Resistant Security Module (TRSM) using the terminal operating system's PCI-certified Secure-Reading and Exchange of Data (SRED) module at the point where card data is captured.
How its Applied	• Integrated with any PIN Pad • Installing TA is hardware agnostic which means it can be applied to numerous certified devices • Encrypts Track 1, Track 2, and Keyed	• Integrated with VeriFone integrated PIN Pads ONLY • Cannot serve at POS or gateway level • Encrypts PAN and Discretionary Data in tamper resistant

TransArmor Encryption Differentiators		
Method	**TransArmor Public Key Infrastructure (PKI)**	**TransArmor VeriFone Edition**
	Data at POS level	hardware
Key Method	Asymmetric Method- Using two keys (Public & Private), TA infrastructure produces a cipher text of 344 bytes of indecipherable code that protects data by transforming into an illegible series of numbers and letters that is easily distinguishable from cardholder data. Public key can only be decrypted by Private key , both of which are safely stored ONLY at First Data	Symmetric Method - The FPE option relies on symmetric encryption keys, i.e., the same key is used to encrypt and decrypt the cardholder data using Advanced Encryption Standard (AES) that uses unique keys per device
Format	344-bytes of data - long prime numbers called keys, only First Data can unlock the public key with the private key	Encrypts data so output is in same length and characters set as input. This type of encryption is called Format-Preserving Encryption (FPE) First 6-digits and last 4-digits left in the clear to allow BIN and routing functions to be performed correctly. It is important to note that TransArmor (RSA) has BIN routing capabilities as well.
Key Management	One key ID per sales channel. Each sales alliance has a specific key ID; therefore, the vendors will have several key IDs depending on the merchant and their merchant acquirer.	One key ID per device. Keys must be 'injected securely' into device at a secure facility, just like that of PIN Debit. This process ensures that the industry required standard of providing split-knowledge and dual-control is met. Keys can be injected via 'VRK/VeriFone Remote Key'. There is a setup process with VeriFone and the process has minimum O/S requirements. There is no specific timeframe or best practice for key rotation for Unique Keys per Device – merchants are encouraged to follow PCI Key Rotation guidelines.

3.1.1 Supported Data Entry Methods—PKI Encryption and Tokenization

The Host and Controller Interface specification supports various card data entry methods for PKI Encryption and Tokenization.

The new sub-element “EDATA Identifier” that is part of Element No. 18 (Card Data) is used to indicate the type of data being processed. For additional information, please refer to chapter 16, “Data Element Descriptions” in the latest version of Host and Controller Interface Specification.

PKI Encryption and Tokenization		
Data Entry Method	**EDATA Identifier**	**Description**
Original Transaction Data—Swiped card	1	Encrypted Track1 data
	2	Encrypted Track2 data
Original Transaction Data—Radio Frequency Identification (RFID) Service	1	Encrypted Track1 data
	2	Encrypted Track2 data
Original Transaction Data—Manually keyed **Note**: Expiration Date (Element No. 127) must be included.	3	Encrypted PAN
Follow-on Transaction Data[1] **Note**: Expiration Date (Element No. 127) must be included.	0	Host-assigned Token

3.2 TransArmor® Tokenization

First Data has two types of tokens available, TransArmor Multi-Pay Tokens and TransArmor Tokens, each with different capabilities, however, all Tokens share the below common characteristics:

- Tokens match the format of the initiating PAN. For example: If the PAN is of 19-digits, the token is also of 19-digits length
- Tokens are unique for major card brands (American Express, Discover, MasterCard, or Visa)
- Tokens do not pass MOD-10 or Luhn checks
- Tokens share the same last 4-digits as those of the corresponding PAN
- Tokens do not expire. The same token follows the card through all the subsequent transactions
- Tokens are card-based. A merchant will always receive a unique token for a specific PAN
- Token Values are non-reversible and not mathematically derived from the initiating PAN
- Tokens can be shared universally or are unique to a merchant (MultiPay Token)

3.2.1 TransArmor® Tokens

TransArmor Tokens are generated at the RSA Safe Proxy within FD's PCI secure environment and returned with the transaction's authorization response to the merchant. Tokens cannot be used to initiate financial transactions. The Token is returned as part of the authorization process and the merchant is able to make adjustments to the transaction until the end of day settlement is sent to First Data.

3.2.2 TransArmor® Multi-Pay Tokens

TransArmor Multi-Pay Tokens address the primary security risk and PCI burden inherent in a Card-Not-Present (CNP) environment—the need to store customer's preferred payment information for subsequent transactions (using the same card)—making them an ideal solution for e-Commerce merchants and service providers with recurring invoices. Multi-Pay Tokens have the same characteristics as TransArmor Token, plus the following additional features:

- Unique to a particular merchant
- Replace cards' PANs in all subsequent transactions (card present and card not present) using the same card – valuable for both POS and e-Commerce/ CNP environments
- Stored in lieu of the PAN to perform transactions for new or recurring payments
- Used for refunds and credits also
- Enables merchants to track buying patterns (buying pattern is used to analyze the sales trends) and launch marketing/loyalty programs while within PCI Compliance
- Supports any business that needs to initiate a financial transaction without card being present

TransArmor Tokenization Differentiators		
Feature	**TransArmor Token**	**Multi-Pay Token**
Technology Partner	RSA (SafeProxy)	RSA (SafeProxy)
Aliases	• Single Use • Former Name: F-Token • Token Type must be “0001”	• Multi–Use • Former Name: R-Token • Token Type is not “0001”
Summary	Process of replacing a PAN with a “token”, a non-sensitive surrogate. The token uniquely represents a customer’s account information, removing the need for merchants to store PAN’s in their card data environment (CDE) Tokenization mitigates security risks associated with storing sensitive card payment data on merchant system	Same as TransArmor Token
Token Assignment	Shared across ALL TransArmor merchants	Unique for each merchant
Format	**Format-preserving**, meaning they match the format and share last four digits of the initiating PAN. If a card is 16 digits in length, Token would be a random set of 12 numbers plus the last 4 digits left in the clear. Tokens are generated and distributed specific to Card, so a merchant will always get the same token back for a specific PAN. Generated to not overlap major brand (Visa, MC, AMEX, Discover) BIN ranges (first digit is 0-2 or 7-9) Do not expire – follows the PAN through the card lifecycle	Same as TransArmor Token
Transactions with Token	• Cannot perform any financial transactions with the token itself • Voids (within same day)	• Supports recurring payments from customer, the merchant can submit a Multi-Pay Token to initiate a sale on a regular basis for recurring transactions without contacting the customer to reconfirm card data • Perform any financial transaction (including credits, returns, and sales)with Token itself

TransArmor Tokenization Differentiators		
Feature	**TransArmor Token**	**Multi-Pay Token**
		Can get Token via a non-financial transaction to place in customer profile for future use • Can only be monetized by the merchant

3.2.3 Supported Data Entry Methods—Token Only

The Host and Controller Interface specification supports various card data entry methods for Token Only transactions.

The new sub-element “EDATA Identifier” that is part of Element No. 18 (Card Data) is used to indicate the type of data being processed. For additional information, please refer to section 16.2 Data Elements in Data Element Number Order in the latest version of Host and Controller Interface Specification.

Token Only		
Data Entry Method	**EDATA Identifier**	**Description**
Original Transaction Data—Swiped card	4	Unencrypted Track1 or Track2 data
Original Transaction Data—Radio Frequency Identification (RFID) Service	4	Unencrypted Track1 or Track2 data
Original Transaction Data—Manually keyed **Note**: Expiration Date (Element No. 127) must be included.	4	Unencrypted PAN
Follow-on Transaction Data **Note**: Expiration Date (Element No. 127) must be included.	0	Host-assigned Token

3.3 Hardware/ Software Requirements

The following information applies to both processing methods.

In order to use TransArmor, a merchant must have the required POS device and the software release—either PKI Encryption and Tokenization or Token Only—that support this feature.

Note: Contact your BUYPASS representative for a current listing of equipment options.

TransArmor is an optional software feature. Vendors developing code to support it must have the capability to enable/disable it.

Merchant participation in TransArmor must be approved by First Data Corporation followed by the necessary certification process. Only then can it be enabled/disabled by the vendor. Please contact your BUYPASS representative for additional information.

Note: Only supported cards can be used for TransArmor. For a list of supported cards, please see section 3.5, “Supported Card Types.”

3.4 Obtaining/Maintaining the Key ID

Note: Obtaining/Maintaining the Key ID can take place only for PKI Encryption and Tokenization processing method.

The following information applies only to PKI Encryption and Tokenization.

Before successful TransArmor processing can occur, the device must have the appropriate Key ID. The device downloads the Key ID following hardware and/or software installation.

TransArmor processing takes place after the Key ID has been downloaded using the TransArmor PKI Key Load process.

The Key ID is maintained under the following circumstances:

- Faulty equipment replacement
- Regular Key ID update schedules
- Nonscheduled Key ID updates as a result of an unsuccessful TransArmor transaction that indicates that a new Key ID and Key are needed

3.5 Supported Card Types

The following card types are supported for both processing methods:

- Credit
- Debit
- Electronic Benefits Transfer (EBT)
  - ◊ Food stamp benefits
  - ◊ Cash benefits
  - ◊ eWIC

3.6 Supported Transaction Types

These specifications support Financial Transaction Requests and Responses for the following transaction types (These transactions have been arranged in groups based on similar transaction flow.) for both processing methods:

Note: Please refer to section 3.7, "Message Format Impacts—PKI Encryption and Tokenization," and section 3.8, " Message Format Impacts—Token Only" for specific message format information.

Supported Transaction Types— Credit Card Transactions	
Transaction Type Code	**Transaction Type**
29	Account Verification (Authorization Only without Hold)
36	Balance Inquiry
40	Purchase
41	Void (Reversal)
42	Merchandise Return
43	Authorization Only Request (approval without capture)
44	Purchase Request after Off-line Approval
45	Request with Prior Voice Authorization (Preauthorized Completion)
46	Off-line Reversal
47	Authorization Only Cancellation
49	Time-out Reversal

Supported Transaction Types— Debit Card Transactions	
Transaction Type Code	**Transaction Type**
29	Account Verification (Authorization Only without Hold)
30	Purchase
31	Reversal (Void)
32	Authorization Only Request (Approval without Capture)

33	Preauthorized Completion
34	Purchase Request after Off-line Approval
35	Resubmission of 34 or 37 Previously Declined Due to Invalid PIN
37	Resubmission of 34 (with PIN and Track 2)
39	Merchandise Return
96	Time-out Reversal
97	Authorization Only Cancellation

Supported Transaction Types— EBT—Food Stamp Transactions	
Transaction Type Code	**Transaction Type**
36	Balance Inquiry
60	Food Stamp Purchase
61	Food Stamp Void (Reversal)
62	Food Stamp Return
69	Food Stamp Time-out Reversal

Supported Transaction Types—EBT—Cash Transactions	
Transaction Type Code	**Transaction Type**
36	Balance Inquiry
70	EBT Cash Purchase
71	EBT Cash Void (Reversal)
79	EBT Cash Time-out Reversal

Supported Transaction Types— Token Registration Transaction	
Transaction Type Code	**Transaction Type**
10	GET-TOKEN-FOR-PAN

3.7 Message Format Impacts—PKI Encryption and Tokenization

The following existing messages are impacted by TransArmor PKI Encryption and Tokenization:

- TransArmor PKI Encryption and Tokenization Authorization Request
- TransArmor PKI Encryption and Tokenization Authorization Response

The following new messages have been added for TransArmor PKI Encryption and Tokenization:

- TransArmor PKI Key and Key ID Load Request
- TransArmor PKI Key and Key ID Load Response

3.7.1 Authorization Request Impacts

An Authorization Request can contain two data areas:

- Required Data Area
- Optional Data Area

3.7.1.1 Required Data Area Impacts—Existing Data Elements

The following existing data elements in the Required Data Area of the Authorization Request are impacted for PKI Encryption and Tokenization:

Notes: For detailed message layout information, please refer to section 15.4.3.1 Required Data Area in the latest version of Host and Controller Interface Specification.

For detailed data element information, please refer to section 16.2 Data Elements in Data Element Number Order in the latest version of Host and Controller Interface Specification.

TransArmor PKI Encryption and Tokenization Authorization Request—Impacts Required Data Area
• Manual Entry Flag (Element No. 47) • Card Data (Element No. 18) • Version Number (Element No. 90) • Optional Area Length (Element No. 53)

3.7.1.2 Required Data Area Impacts—New Data Elements

There are no new elements for PKI Encryption and Tokenization Processing in the Required Data Area.

3.7.1.3 Optional Data Area Impacts—Existing Data Elements

There are no impacted data elements in the Optional Data area for PKI Encryption and Tokenization.

3.7.1.4 Optional Data Area Impacts—New Data Elements

There are two new data elements in the Optional Data area for PKI Encryption and Tokenization:

Notes: For detailed message layout information, please refer to section 15.4.3.2 Optional Data Area in the latest version of Host and Controller Interface Specification.

For detailed data element information, please refer to section 16.2 Data Elements in Data Element Number Order in the latest version of Host and Controller Interface Specification.

TransArmor PKI Encryption and Tokenization Authorization Request—Impacts Optional Data Area
• EDATA (Element No. 126) • Expiration Date (Element No. 127)

3.7.2 Authorization Response Impacts

An Authorization Response contains two data areas:

- Required Data Area
- Optional Data Area

3.7.2.1 Required Data Area Impacts—Existing Data Elements

The following existing data elements in the Required Data Area of the Authorization Response are impacted for PKI Encryption and Tokenization:

Notes: For detailed message layout information, please refer to section 15.4.4.1 Required Data Area in the latest version of Host and Controller Interface Specification.

For detailed data element information, please refer to section 16.2 Data Elements in Data Element Number Order in the latest version of Host and Controller Interface Specification.

TransArmor PKI Encryption and Tokenization Authorization Response—Impacts Required Data Area
• Card Data (Element No. 18) • Terminal Display (Element No. 80 • Version Number (Element No. 90) • Optional Area Length (element No. 53)

3.7.2.2 Required Data Area Impacts—New Data Elements

There are no new data elements in the Required Data area for PKI Encryption and Tokenization.

3.7.2.3 Optional Data Area Impacts—Existing Data Elements

There are no impacts to existing data elements in the Optional Data area for PKI Encryption and Tokenization.

3.7.2.4 Optional Data Area Impacts—New Data Elements

There are two new data elements in the Optional Data area for PKI Encryption and Tokenization:

Notes: For detailed message layout information, please refer to section 15.4.4.2 Optional Data Area in the latest version of Host and Controller Interface Specification.

For detailed data element information, please refer to section 16.2 Data Elements in Data Element Number Order in the latest version of Host and Controller Interface Specification.

TransArmor PKI Encryption and Tokenization Authorization Response—Impacts Optional Data Area
• Download Indicator (Element No. 128) • Key ID (Element No. 129)

3.7.3 Key and Key ID Load Request

The Key and Key ID Load Request is a new message for TransArmor PKI Encryption and Tokenization. It is used to request a new TransArmor PKI Key and Key ID.

Note: Key and Key ID loads must be supported when using TransArmor PKI Encryption and Tokenization method.

The following existing data elements must be present with the appropriate TransArmor PKI Encryption and Tokenization information for this message:

Notes: For detailed message layout information, please refer to section 3.9.1.1 Request in this document.

For detailed data element information, please refer to section 16.2 Data Elements in Data Element Number Order in the latest version of Host and Controller Interface Specification.

TransArmor PKI Encryption and Tokenization Key and Key ID Load Request
• Record Type (Element No. 61) • Device ID (Element No. 33) • Sequence Number (Element No.63) • Transaction Date (Element No. 86) • Transaction Time (Element No. 87) • Terminal Number (Element No. 81) • Firmware Version (Element No. 40) • Hardware Version (Element No. 44) • Software Version (Element No. 64)

3.7.4 Key and Key ID Load Response

The Key and Key ID Load Response is a new message for TransArmor PKI Encryption and Tokenization. It is used to return a new TransArmor PKI Key and Key ID.

Note: Key and Key ID loads must be supported when using TransArmor PKI Encryption and Tokenization method.

The following existing data elements must be present with the appropriate TransArmor PKI Encryption and Tokenization information for this message:

Notes: For detailed message layout information, please refer to section 3.9.1.2 Response in this document.

For detailed data element information, please refer to section 16.2 Data Elements in Data Element Number Order in the latest version of Host and Controller Interface Specification.

TransArmor PKI Encryption and Tokenization Key and Key ID Load Response Impacted Data Elements
• Record Type (Element No. 61) • Device ID (Element No. 33) • Sequence Number (Element No.63) • Transaction Date (Element No. 86) • Transaction Time (Element No. 87) • Terminal Number (Element No. 81) • Response Code (Element No. 62) • Optional Area Length (Element No. 53)

The following new data elements must be present with the appropriate TransArmor PKI Encryption and Tokenization information for this new message:

Notes: For detailed message layout information, please refer to section 3.9.1.2 Response in this document.

For detailed data element information, please refer to section 16.2 Data Elements in Data Element Number Order in the latest version of Host and Controller Interface Specification.

TransArmor PKI Encryption and Tokenization Key and Key ID Load Response New Data Elements
• Key ID (Element No. 129) • Key Data (Element No. 130)

3.8 Message Format Impacts—Token Only

The following is the new message specific to TransArmor Multi-Pay Token transactions:

- TransArmor Token Registration (GET-TOKEN-FOR-PAN)

The following existing messages are impacted by TransArmor Token Only:

- TransArmor Token Only Authorization Request
- TransArmor Token Only Authorization Response

3.8.1 Authorization Request Impacts

An Authorization Request can contain two data areas:

- Required Data Area
- Optional Data Area

3.8.1.1 Required Data Area Impacts—Existing Data Elements

The following existing data elements in the Required Data Area of the Authorization Request are impacted for Token Only:

Notes: For detailed message layout information, please refer to section 15.4.3.1 Required Data Area in the latest version of Host and Controller Interface Specification.

For detailed data element information, please refer to section 16.2 Data Elements in Data Element Number Order in the latest version of Host and Controller Interface Specification.

TransArmor Token Only Authorization Request—Impacts Required Data Area
• Manual Entry Flag (Element No. 47) • Card Data (Element No. 18) • Version Number (Element No. 90)

3.8.1.2 Required Data Area Impacts—New Data Elements

There are no new elements in the Required Data Area for Token Only Processing.

3.8.1.3 Optional Data Area Impacts—Existing Data Elements

There are no impacted data elements in the Optional Data area for Token Only Processing.

3.8.1.4 Optional Data Area Impacts—New Data Elements

There are two new data elements in the Optional Data area for Token Only Processing:

Notes: For detailed message layout information, please refer to section 15.4.3.2 Optional Data Area in the latest version of Host and Controller Interface Specification.

For detailed data element information, please refer to section 16.2 Data Elements in Data Element Number Order in the latest version of Host and Controller Interface Specification.

TransArmor Token Only Authorization Request—Impacts Optional Data Area
• EDATA (Element No. 126) • Expiration Date (Element No. 127)

3.8.2 Authorization Response Impacts

An Authorization Response contains two data areas:

- Required Data Area
- Optional Data Area

3.8.2.1 Required Data Area Impacts—Existing Data Elements

The following existing data elements in the Required Data Area of the Authorization Response are impacted for Token Only:

Notes: For detailed message layout information, please refer to section 15.4.4.1 Required Data Area in the latest version of Host and Controller Interface Specification.

For detailed data element information, please refer to section 16.2 Data Elements in Data Element Number Order in the latest version of Host and Controller Interface Specification.

TransArmor Token Only Authorization Response—Impacts Required Data Area
• Card Data (Element No. 18) • Terminal Display (Element No. 80 • Version Number (Element No. 90)

3.8.2.2 Required Data Area Impacts—New Data Elements

There are no new data elements in the Required Data area for Token Only.

3.8.2.3 Optional Data Area Impacts—Existing Data Elements

There are no impacts to existing data elements in the Optional Data area for Token Only.

3.8.2.4 Optional Data Area Impacts—New Data Elements

There are two new data elements in the Optional Data area for Token Only:

Notes: For detailed message layout information, please refer to section 15.4.4.2 Optional Data Area in the latest version of Host and Controller Interface Specification.

For detailed data element information, please refer to section 16.2 Data Elements in Data Element Number Order in the latest version of Host and Controller Interface Specification.

TransArmor Token Only Authorization Response—Impacts Optional Data Area
• Download Indicator (Element No. 128) • Key ID (Element No. 129)

3.9 TransArmor® Message Formats

3.9.1 TransArmor® PKI Key and Key ID Load

This section contains request and response message formats for a TransArmor PKI Key and Key ID Load.

Note: The Token Only processing method does not require a TransArmor PKI Key Load Request.

3.9.1.1 Request

The following table contains format information about the TransArmor PKI Key and Key ID Load Request:

Note: There are no Field Separators in this message.

Message Format **TransArmor PKI Key and Key ID Load Request**						
Field No.	**Element No.**	**Element Name**	**Pos.**	**Max. Len.**	**Entry is: R/O/C[1]**	**Description**
1	61	Record Type	1	3	R	Identifies the message type. **Fixed value**: STQ **Source**: Device
2	33	Device ID	4	11	R	Identifies a merchant device. **Source**: Device
3	63	Sequence Number	15	6	R	Identifies the unique transaction identifier. **Source**: Device
4	86	Transaction Date	21	6	R	Identifies the transaction's creation date. **Source**: Device
5	87	Transaction Time	27	6	R	Identifies the transaction's creation time. **Source**: Device
6	81	Terminal Number	33	13	R	Identifies the transaction device by Device Type, State Code, BUYPASS Merchant Number, and Device Number. For TransArmor, the first two characters (Device Type) of this element's value must be "++" regardless of the actual device type. **Source**: Device
7	40	Firmware Version	46	8	R	Identifies the current version of the device's firmware. **Source**: Device
8	44	Hardware Version	54	4	R	Identifies the version number of the device's hardware level. **Source**: Device

Message Format TransArmor PKI Key and Key ID Load Request						
Field No.	**Element No.**	**Element Name**	**Pos.**	**Max. Len.**	**Entry is: R/O/C[1]**	**Description**
9	64	Software Version	58	8	R	Identifies the version number of the device's software application. **Source**: Device

[1]Required/Optional/Conditional

3.9.1.2 Response

The following table contains format information about the TransArmor PKI Key and Key ID Load Response:

Note: There are no Field Separators in this message.

Message Format TransArmor PKI Key and Key ID Load Response						
Field No.	**Element No.**	**Element Name**	**Pos.**	**Max. Len.**	**Entry is: R/O/C[1]**	**Description**
1	61	Record Type	1	3	R	Identifies the message type. **Fixed value**: STP **Source**: Host
2	33	Device ID	4	11	R	Identifies a merchant device. **Source**: Request
3	63	Sequence Number	15	6	R	Identifies the unique transaction identifier. **Source**: Request
4	86	Transaction Date	21	6	R	Identifies the transaction's creation date. **Source**: Request
5	87	Transaction Time	27	6	R	Identifies the transaction's creation time. **Source**: Request
6	81	Terminal Number	33	13	R	Identifies the transaction device by Device Type, State Code, BUYPASS Merchant Number, and Device Number. For TransArmor, the first two characters (Device Type) of this element's value must be "++" regardless of the actual device type. **Source**: Request
7	1	Action Code	46	1	R	Identifies an approval or decline and class of decline. **Source:** Authorizer or BUYPASS
8	62	Response Code	47	2	R	Indicates an approved/declined transaction. **Source**: Host
9	53	Optional Area Length	49	3	R	Identifies the Key ID associated with the included encryption Key. **Source**: Host
10	129	Key ID	52	11	R	Identifies the Key ID associated with the included encryption Key. **Source**: Host

Message Format TransArmor PKI Key and Key ID Load Response						
Field No.	**Element No.**	**Element Name**	**Pos.**	**Max. Len.**	**Entry is: R/O/C[1]**	**Description**
11	130	Key Data	63	400	R	Identifies the new encryption Key or the Error Message. **Source**: Host

[1]Required/Optional/Conditional

3.9.2 TransArmor® Signing Key and Signed Key ID Load

This section contains request and response message formats for a Signed TransArmor Key and Key ID Load.

3.9.2.1 Request

The following table contains format information about the Signed TransArmor Key and Key ID Load Request:

Note: There are no Field Separators in this message.

Message Format **Signing Key ID Load and Signed TransArmor Key Request**						
Field No.	**Element No.**	**Element Name**	**Pos.**	**Max. Len.**	**Entry is: R/O/C[1]**	**Description**
1	61	Record Type	1	3	R	Identifies the message type. **Fixed value**: SSQ **Source**: Device
2	33	Device ID	4	11	R	Identifies a merchant device. **Source**: Device
3	63	Sequence Number	15	6	R	Identifies the unique transaction identifier. **Source**: Device
4	86	Transaction Date	21	6	R	Identifies the transaction's creation date. **Source**: Device
5	87	Transaction Time	27	6	R	Identifies the transaction's creation time. **Source**: Device
6	81	Terminal Number	33	13	R	Identifies the transaction device by Device Type, State Code, BUYPASS Merchant Number, and Device Number. For TransArmor, the first two characters (Device Type) of this element's value must be "++" regardless of the actual device type. **Source**: Device
7	40	Firmware Version	46	8	R	Identifies the current version of the device's firmware. **Source**: Device
8	44	Hardware Version	54	4	R	Identifies the version number of the device's hardware level. **Source**: Device

Message Format Signing Key ID Load and Signed TransArmor Key Request						
Field No.	**Element No.**	**Element Name**	**Pos.**	**Max. Len.**	**Entry is: R/O/C[1]**	**Description**
9	53	Optional Area Length	58	3	R	Identifies the length of following optional data fields. **Source**: Device
10	129	Key ID	61	11	R	Identifies the Signing Key ID loaded into the POS device. Optional tag id "@" **Source:** Host **Note:** This data element is used in the Signed Key ID Load request only.

[1]Required/Optional/Conditional

3.9.2.2 Response

The following table contains format information about the TransArmor Key and Key ID Load Response:

Note: There are no Field Separators in this message.

Message Format **Signing Key ID Load and Signed TransArmor Key Response**						
Field No.	**Element No.**	**Element Name**	**Pos.**	**Max. Len.**	**Entry is: R/O/C[1]**	**Description**
1	61	Record Type	1	3	R	Identifies the message type. **Fixed value**: SSP **Source**: Host
2	33	Device ID	4	11	R	Identifies a merchant device. **Source**: Request
3	63	Sequence Number	15	6	R	Identifies the unique transaction identifier. **Source**: Request
4	86	Transaction Date	21	6	R	Identifies the transaction's creation date. **Source**: Request
5	87	Transaction Time	27	6	R	Identifies the transaction's creation time. **Source**: Request
6	81	Terminal Number	33	13	R	Identifies the transaction device by Device Type, State Code, BUYPASS Merchant Number, and Device Number. For TransArmor, the first two characters (Device Type) of this element's value must be "++" regardless of the actual device type. **Source**: Request
7	1	Action Code	46	1	R	Identifies an approval or decline and class of decline. **Source:** Authorizer or BUYPASS
8	62	Response Code	47	2	R	Indicates an approved/declined transaction. 00 = Approved 2D = Declined, not TransArmor merchant or invalid CA-ID **Source**: Host
9	53	Optional Area Length	49	3	R	Identifies the Length of following optional data fields. **Source**: Host

Message Format Signing Key ID Load and Signed TransArmor Key Response						
Field No.	**Element No.**	**Element Name**	**Pos.**	**Max. Len.**	**Entry is: R/O/C[1]**	**Description**
10	129	Key ID	52	11	R	Identifies the Key ID associated with the included encryption Key. Optional tag id "@" **Source**: Host
11	130	Key Data	63	999	R	Identifies the new encryption Key or the Error Message. Optional tag id "#" **Source**: Host

[1]Required/Optional/Conditional

3.10 Receipt Requirements

In addition to the receipt requirements described in section 12.1.8 "Receipt Requirements" in the latest version of Host and Controller Interface Specification, the following TransArmor requirement is necessary:

- The masked number printed on all receipts is the masked token. The last four digits of the token are the same as the last four digits of the card's PAN.

3.11 TransArmor® - VeriFone Edition Processing

First Data and VeriFone Systems, Inc. are working together to offer a VeriFone edition of the First Data TransArmor solution to US multi-lane and petroleum merchants. This will enable businesses using VeriFone Mx devices and other devices to take advantage of a complete security solution combining VeriFone's encryption along with tokenization technology from RSA, the Security Division of EMC Corporation.

Note: Contact your BUYPASS representative for a current listing of device options.

Please refer to the following new information about TransArmor - VeriFone edition processing (TA-VE) in the latest version of Host and Controller Interface Specification:

- Section 15.4.3.2, "Optional Data Area" (Authorization Request)
- Section 15.4.4.2, "Optional Data Area" (Authorization Response)

Please refer to the following new information about TransArmor - VeriFone edition processing (TA-VE) in this document:

- Element No. 18 (Card Data)
- Element No. 53 (Optional Area Length)
- Element No. 127 (Expiration Date)
- Element No. 134 (Settlement ID)

3.11.1 Registering a Terminal for VeriFone Encryption

In order to use TransArmor VeriFone encryption, the device must first be registered by initiating a Registration event which activates the VeriFone encryption on the terminal and registers the device with the encryption/decryption server.

3.11.1.1 Device Registration

Device Registration refers to the process of using the "RegiStart" Card or RegiStart administrative function coded for the POS. This enables encryption on the device and registers the device with the encryption/decryption server. The RegiStart Card (or function) is encoded with Track 3 data unique to the Merchant's boarding information and the device configuration file. The encrypted PAN of the RegiStart card/function is 15 digits (within ISO standards). Additionally, the BIN is 515111.

3.11.1.2 Registration Process

- Ensure the device is connected to the point of sale and powered on.
- Initiate a $1.00 MasterCard Sale transaction with the payment application and swipe the RegiStart Card or initiate the RegiStart administrative function coded on the POS. The transaction should be sent using the same TAP information as will be used when sending normal transactions.
- The MasterCard Sale transaction is formatted and message is preserved as Track 1 and Track 2 data.
- Buypass sends the transaction to the decryption server.
- The Terminal ID is registered with the decryption server during the registration process.
- The MasterCard Sale transaction Response Code is sent back to the merchant.
- The device is now registered and is in an encrypting state ready to encrypt transactions.

3.11.1.3 Device Movement

When a device moves from one lane to another, whether previously encrypting or not, or is brand new out of the box, that device must be re-registered. Re-register the device by performing the steps listed above in the Registration Process. For more information, please contact your account representative.

4. TransArmor® CA Certificate Overview

First Data has implemented the TransArmor (TA) Certificate Authority (CA) solution to handle key exchange for vendor POS terminals and VARs. Certificate Authority solution will enable First Data to validate the source of the public keys.

The standard approach to key delivery is to use a signed X.509 Certificate. The salient features of PKI are listed below:

- First Data sends the Public Data Encryption Keys (DEK) to the merchant through X.509 signed security certificates. The keys are embedded in those certificates.
- The POS terminal is embedded with a CA Certificate chain, so that it can verify and validate the signed DEK.
- Upon initialization, the POS terminals download these signed certificates.

Note: The CA Certificate chain includes the following:

- Signing Key Certificate
- Signed Key Certificate

4.1 Certificate Authority Security Components

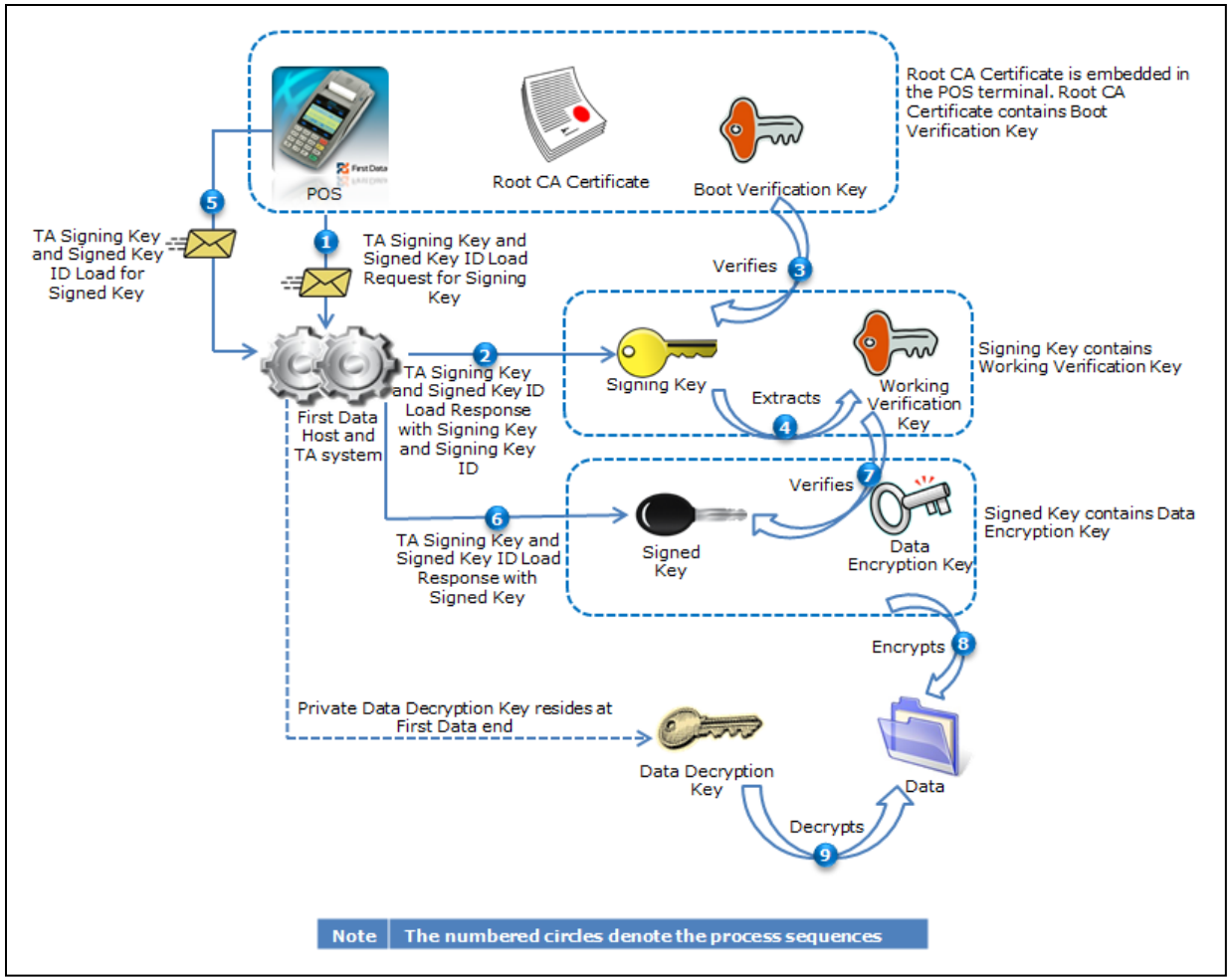
The following security key components are required at the terminal in order to support the enhanced TA secure key exchange process.

- Root CA Certificate
- Boot Verification Key (public)
- Signing Key (private)
- Working Verification Key (public)
- Signing Key ID
- Signed Key
- Data Encryption Key (public)
- Data Encryption Key ID
- Data Decryption Key (private)

Component	Description and Usage
Root CA Certificate	X.509 certificate that contains the Boot Verification Key. The duration of validity is defined in the Certificate.
Boot Verification Key (public)	Public key derived from the Root CA Certificate embedded in the POS device. It is created by First Data Root CA. It used to validate the signature on the Signing Key, in order to unlock the Working Signing Key.
Signing Key (private)	Private key associated with the Working Verification Key (public key). This key is used to sign the Signed Key. It is created by First Data Intermediate Certificate Authority.
Working Verification Key (public)	Derived at POS device from the Signing Key. It is used to validate the signature on the Signed Key which unlocks the Data Encryption Key (DEK).
Signing Key ID	Key ID associated with the Working Signing Key/Working Verification Key private/public key pair. It is sent in request for the Data Encryption Key (DEK) to indicate that the host should send the DEK in an X.509 certificate rather than unsigned.
Signed Key	Key that contains the Data Encryption Key (public). It is signed using the Working Signing Key (private).It is validated using the Working Verification Key (public). The duration of validity is defined in the Certificate. It is downloaded during TransArmor configuration along with the Data Encryption Key ID (DE_ID).
Data Encryption Key (public)	Public key associated with private Data Decryption Key. It is derived at the POS device from the Signed Key. It is used to encrypt the cardholder sensitive data at the POS device.
Data Encryption Key ID	Key ID associated with the Data Decryption Key/Data Encryption Key private/public key pair. It is sent with encrypted data to indicate the Data Decryption Key that must be used to decrypt the data.
Data Decryption Key (private)	Private keys are held by First Data and associated with public Data Encryption Key. It is used to decrypt the cardholder sensitive data at the First Data host.

4.2 TransArmor® CA Key Exchange Process Flow

The following diagram represents the TA CA security keys exchange process.



1) The POS device sends a TA Signing Key and Signed Key ID Load message requesting for Signing Key.
2) The POS device receives the Signing Key in the TA Signing Key and Signed Key ID Load response from First Data.
3) The POS device uses the Boot Verification Key to validate the Signing Key.
4) After the Signing Key is validated, the Boot Verification Key extracts the Working Verification Key from the Signing Key.
5) The POS device sends a TA Signing Key and Signed Key ID Load message requesting for Signed Key using the Signing Key ID.
6) The POS device receives the Signed Key in the TA Signing Key and Signed Key ID Load response from First Data.
7) The POS device uses the Working Verification Key to validate the Signed Key.
8) After the Signed Key is validated, the Working Verification Key extracts the DEK.
9) The DEK is used to encrypt the sensitive cardholder data in the TA authorization request.

Note:

- The Root CA Certificate is embedded in the POS terminal.
- The POS terminal extracts the Boot Verification Key from the Root CA Certificate.
- The Root CA is securely managed by the encrypting device and is delivered outside of the message specification.
- If you receive E2D in the Action Code and Response Code fields in step 2 or 6, restart the key exchange from step 1.

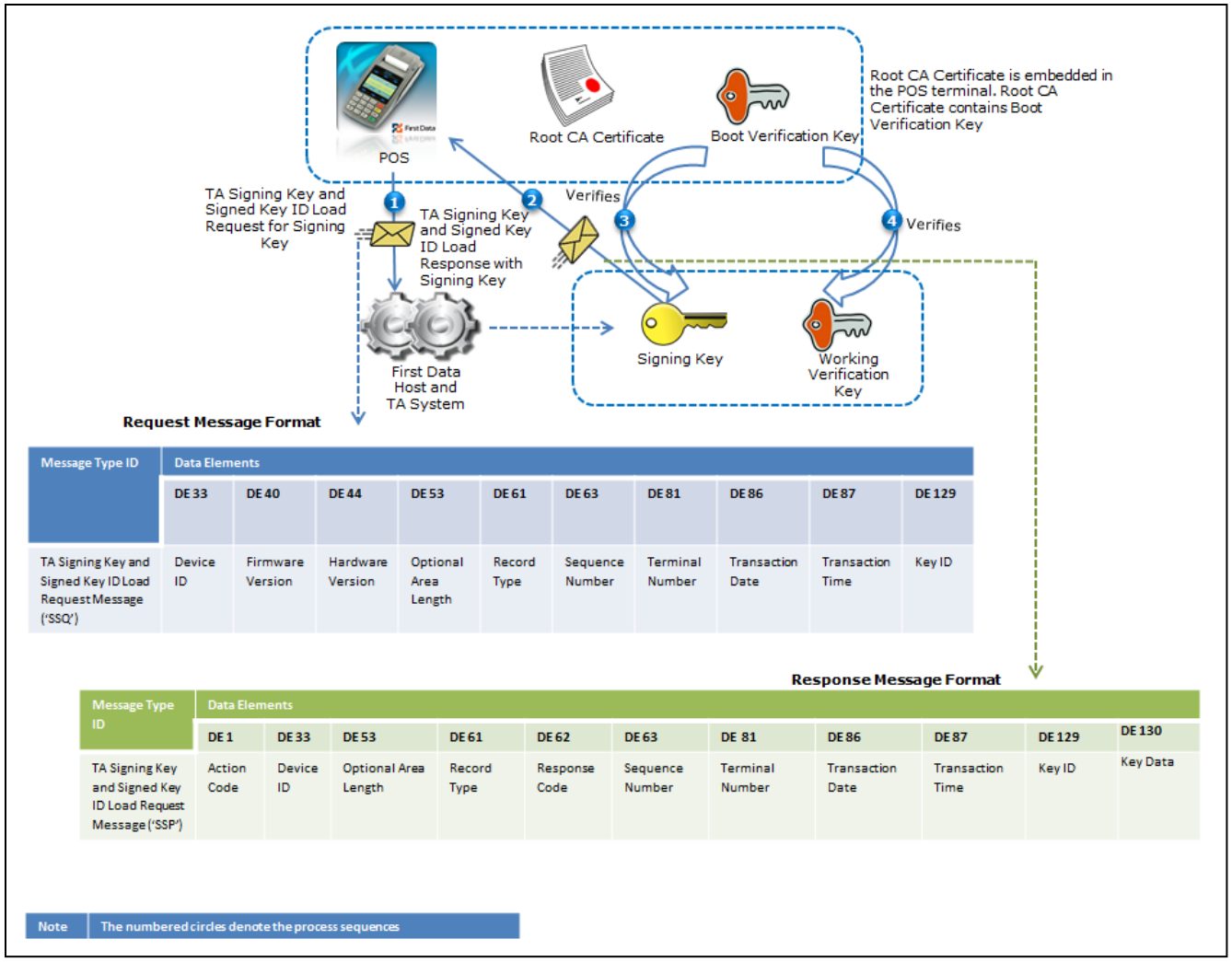
4.3 TransArmor® (with Signed Key) Initialization Process Flow

If the terminal vendor has embedded root key and is enabled for Certificate Authority, then the initialization process is as follows below:

Note:

- The Root CA Certificate is embedded in the application download package
- The Root CA Certificate contains the public Boot Verification Key

4.3.1.1.1 *Step 1: Request and Response for Signing Key Certificate*



Request Message Format

Message Type ID	Data Elements									
	DE 33	DE 40	DE 44	DE 53	DE 61	DE 63	DE 81	DE 86	DE 87	DE 129
TA Signing Key and Signed Key ID Load Request Message ('SSQ')	Device ID	Firmware Version	Hardware Version	Optional Area Length	Record Type	Sequence Number	Terminal Number	Transaction Date	Transaction Time	Key ID

Response Message Format

Message Type ID	Data Elements										
	DE 1	DE 33	DE 53	DE 61	DE 62	DE 63	DE 81	DE 86	DE 87	DE 129	DE 130
TA Signing Key and Signed Key ID Load Request Message ('SSP')	Action Code	Device ID	Optional Area Length	Record Type	Response Code	Sequence Number	Terminal Number	Transaction Date	Transaction Time	Key ID	Key Data

Note	The numbered circles denote the process sequences

1. The POS device sends a TA Signing Key and Signed Key ID Load message requesting for Signing Key.

2. The POS device receives the Signing Key in the TA Signing Key and Signed Key ID Load response from First Data.

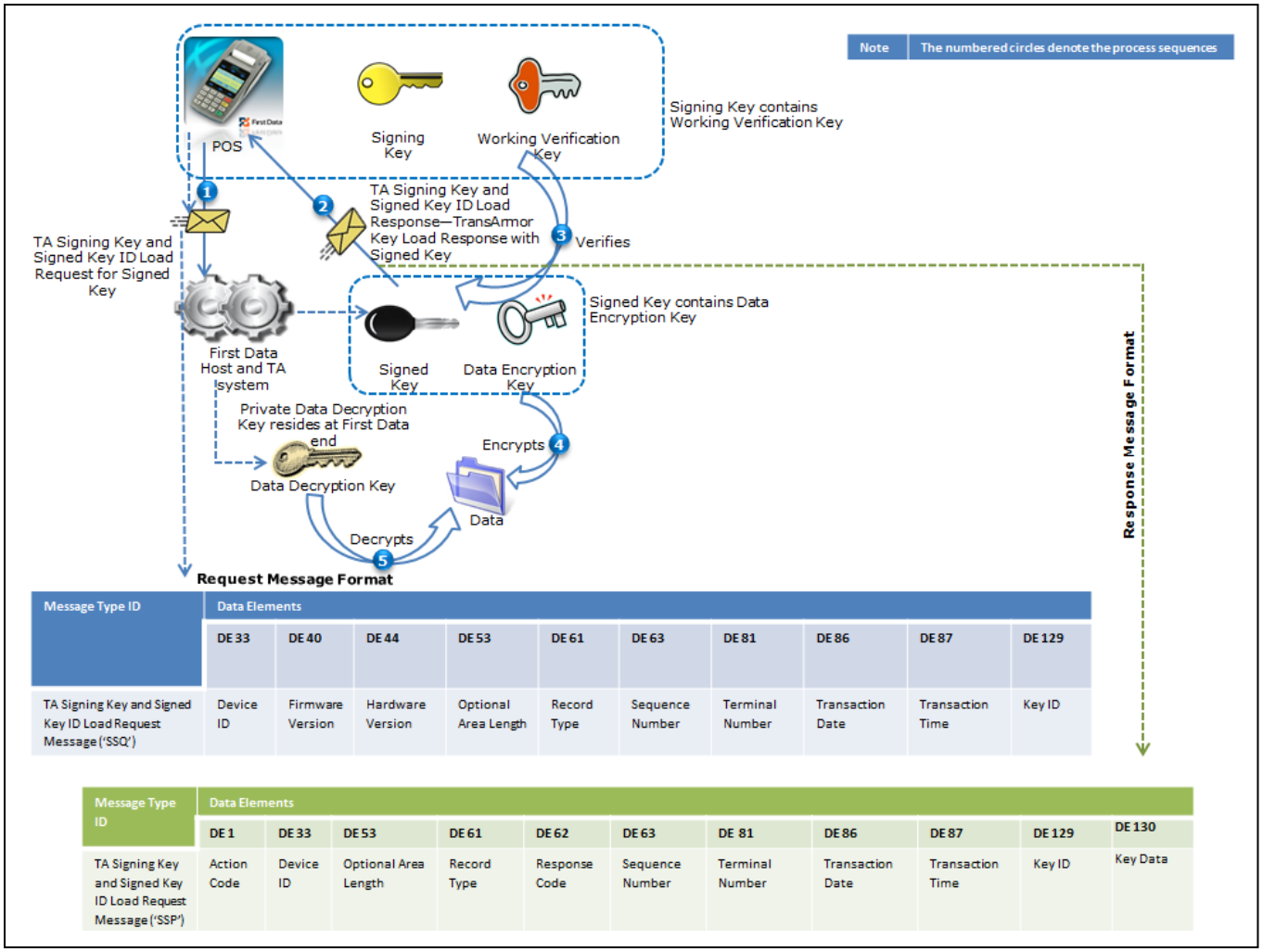
Note: In the TA Key and Key ID Load Response Message:
- Data Element 129 (Key ID) contains the Signing Key ID
- Data Element 130 (Key Data) contains the Signing Key Data

3. The POS device uses the Boot Verification Key to validate the Signing Key.

4. After the Signing Key is validated, the Boot Verification Key validates the Working Verification Key.

Note: The Signing Key contains the Working Verification Key.

4.3.1.1.2 *Step 2: Request and Response for Signed Key Certificate*



Message Type ID	Data Elements									
	DE 33	DE 40	DE 44	DE 53	DE 61	DE 63	DE 81	DE 86	DE 87	DE 129
TA Signing Key and Signed Key ID Load Request Message ('SSQ')	Device ID	Firmware Version	Hardware Version	Optional Area Length	Record Type	Sequence Number	Terminal Number	Transaction Date	Transaction Time	Key ID

Message Type ID	Data Elements										
	DE 1	DE 33	DE 53	DE 61	DE 62	DE 63	DE 81	DE 86	DE 87	DE 129	DE 130
TA Signing Key and Signed Key ID Load Request Message ('SSP')	Action Code	Device ID	Optional Area Length	Record Type	Response Code	Sequence Number	Terminal Number	Transaction Date	Transaction Time	Key ID	Key Data

1. The POS device sends a TA Signing Key and Signed Key ID Load requesting for Signed Key.

Note: In the TA Signing Key and Signed Key ID Load Request Message:

- Data Element 129 (Key ID) contains the Signing Key ID

2. The POS device receives the Signed Key in the TA Signing Key and Signed Key ID Load response from First Data.

Note: In the TA Signing Key and Signed Key ID Load Response Message:

- Data Element 129 (Key ID) contains the Signed Key ID
- Data Element 130 (Key Data) contains the Signed key Data

3. The POS device uses the Working Verification Key to validate the Signed Key.

4. After the Signed Key is validated, the Working Verification Key validates the Data Encryption Key (DEK).
5. The DEK is used to encrypt the sensitive cardholder data in the TA authorization request.
6. First Data uses the Data Decryption Key (DDK) ID to decrypt the encryption block.

Certificate Authority Key Rotation

- First Data notifies the terminals that they are required to update DEK. The notification comes through value '9' of Download Indicator (Data Element 128) and is received by the terminal
- If the Signing Key ID sent in a request does not match the one that First Data expects, the terminals must download new encryption key
- The CA Certificates and the DEK have an expiration date after which they are no longer accepted by First Data and the transactions would be declined
- If you receive E2D in the Action Code and Response Code fields in the response to a TA Key and Key ID Load Request Message, you must restart the Key Exchange process from Step 1.

5. Impacted Data Elements

This section describes the existing data elements impacted by TransArmor processing:

- Action Code (Element No. 1)
- Card Data (Element No. 18)
- Device ID (Element No. 33)
- Firmware Version (Element No. 40)
- Hardware Version (Element No. 44)
- Manual Entry Flag (Element No. 47)
- Optional Area Length (Element No. 53)
- Record Type (Element No. 61)
- Response Code (Element No. 62)
- Sequence Number (Element No. 63)
- Software Version (Element No. 64)
- Terminal Display (Element No. 80)
- Terminal Number (Element No. 81)
- Total Amount (Element No. 82)
- Total Count (Element No. 83)
- Transaction Date (Element No. 86)
- Transaction Time (Element No. 87)
- ECA/TeleCheck® Amount (Element No. 113)
- ECA/TeleCheck® Count (Element No. 114)
- eWIC Count (Element No. 124)
- eWIC Amount (Element No. 125)
- EDATA (Element No. 126)
- Expiration Date (Element No. 127)
- Download Indicator (Element No. 128)
- Key ID (Element No. 129)
- Key Data (Element No. 130)
- Settlement ID (Element No. 134)

Number:	1	**Name:**	Action Code
Character Type:	AN	**Length:**	1 byte

R/O/C:	Required	
Representation:	One uppercase letter or zero	
Purpose:	Identifies a decision made by a card authorizer or BUYPASS about the transaction.	
Processing Rules:	Indicates whether the transaction is approved or declined.	
Valid Codes/Values:	**Codes**	**Description**
	0	Approval with no data capture
	A	Approval with data capture
	C	Call card issuer
	D	Declined by authorizer
	E	System error

Number:	18	**Name:**	Card Data
Character Type:	ANS	**Length:**	

Non-TransArmor (all transactions): 40 bytes

TransArmor (both methods): 40 bytes

TransArmor - VeriFone Edition:

Encryption & Tokenization:

All Requests

All Responses

R/O/C: Required

Representation: Left-aligned; space filled

Non-TransArmor—Initial Transaction—Request and Response:

Format: A variable length (up to 40 bytes) of card data

Non-TransArmor—Follow-on Transaction—Request and Response:

Format: A variable length (up to 40 bytes) of card data

Representation:

TransArmor (PKI Encryption and Tokenization)—Initial Transaction—Request:

Format: TAPnnnnnnxyyyyyyyyyyyzzzz

Where:

TAP = 3-byte TransArmor Indicator

Valid value: TAP

nnnnnn = 6-byte Sequence Number of the transaction that matches the value in Element No. 63 (Sequence Number)

x = 1-byte EDATA (Element No. 126) Identifier

Valid values:
0 – Token
1 – Track1
2 – Track2
3 – PAN (keyed)
4 – Nonencrypted data

yyyyyyyyyyy = 11-byte Key ID

zzzz = 4-byte Token Type ID

Valid value: XXXX = Single use or MultiPay Token; 4-byte alphanumeric value assigned by First Data

TransArmor (PKI Encryption and Tokenization)—Initial Transaction—Response:

Format: TAPnnnnnnxyyyyyyyyyyyzzzz

Where:

"TAPnnnnnnxyyyyyyyyyyyzzzz" is echoed from the original transaction if a time-out occurs before BUYPASS is able to retrieve a token.

or TOKEN

Where: "TOKEN" is the token associated with the PAN transmitted in the original request.

Note: The last four bytes of the token are the same as the PAN's last four bytes. Do not perform a mod10 check routine on the Token.

Representation (*continued*):

TransArmor (PKI Encryption and Tokenization)—Follow-on Transaction— Request:

Format: TAPnnnnnnxyyyyyyyyyyyzzzz

Where:

TAP = 3-byte TransArmor Indicator

Valid value: TAP

nnnnnn = 6-byte Sequence Number of the transaction that matches the value in Element No. 63 (Sequence Number)

x = 1-byte EDATA (Element No. 126) Identifier

Valid value: 0 = Token

yyyyyyyyyyy = 11-byte Key ID

zzzz = 4-byte Token Type ID

Valid value: XXXX = Single use or MultiPay Token; 4-byte alphanumeric value assigned by First Data

Note: The Token is contained in Field No. 15 (Optional Data Area, p. 15-13) in Element No. 126 (EDATA).

TransArmor (PKI Encryption and Tokenization)—Follow-on Transaction—Response:

Format: TAPnnnnnnxyyyyyyyyyyyzzzz

Where: "TAPnnnnnnxyyyyyyyyyyyzzzz" is echoed from the original transaction if a time-out occurs before BUYPASS is able to retrieve a token.

or TOKEN

Where: "TOKEN" is the token associated with the PAN transmitted in the original request.

Note: The last four bytes of the token are the same as the PAN's last four bytes. Do not perform a mod10 check routine on the Token.

Representation (*continued*):

TransArmor (Token Only)—Initial Transaction—Request:

Format: TAPnnnnnnxyyyyyyyyyyyzzzz

Where:

TAP = 3-byte TransArmor Indicator

Valid value: TAP

nnnnnn = 6-byte Sequence Number of the transaction that matches the value in Element No. 63 (Sequence Number)

x = 1-byte EDATA (Element No. 126) Identifier

Valid value:

4 – Nonencrypted data (Track1, Track2, manually-keyed PAN)

yyyyyyyyyyy = zero-filled 900000000000) (**Note**: A Key ID only applies when encrypted data is sent.)

zzzz = 4-byte Token Type ID

Valid value: XXXX = Single use or MultiPay Token; 4-byte alphanumeric value assigned by First Data

TransArmor (Token Only)—Initial Transaction—Response:

Format: TAPnnnnnnxyyyyyyyyyyyzzzz

Where: "TAPnnnnnnxyyyyyyyyyyyzzzz" is echoed from the original transaction if a time-out occurs before BUYPASS is able to retrieve a token.

or TOKEN

Where: "TOKEN" is the token associated with the PAN transmitted in the original request.

Note: The last four bytes of the token are the same as the PAN's last four bytes. Do not perform a mod10 check routine on the Token.

Representation (*continued*):

TransArmor (Token Only)—Follow-on Transaction—Request:

Format: TAPnnnnnnxyyyyyyyyyyyzzzz

Where:

TAP = 3-byte TransArmor Indicator

Valid value: TAP

nnnnnn = 6-byte Sequence Number of the transaction that matches the value in Element No. 63 (Sequence Number)

x = 1-byte EDATA (Element No. 126) Identifier

Valid value: 0 – Token

yyyyyyyyyyy = zero-filled 900000000000) (**Note**: A Key ID only applies when encrypted data is sent.)

zzzz = 4-byte Token Type ID

Valid value: XXXX = Single use or MultiPay Token; 4-byte alphanumeric value assigned by First Data

Note: The Token is contained in Field No. 15 (Optional Data Area, p. 15-13) in Element No. 126 (EDATA).

TransArmor (Token Only)—Follow-on Transaction—Response:

Format: Variable length of up to 40 is echoed from the original transaction if a time-out occurs before BUYPASS is able to retrieve a token.

or TOKEN

Where: "TOKEN" is the token associated with the PAN transmitted in the original request.

Note: The last four bytes of the token are the same as the PAN's last four bytes. Do not perform a mod10 check routine on the Token.

Purpose: Non-TransArmor: Identifies the card or check data used for authorization. TransArmor (Both Processing Methods): Identifies the 25-byte TransArmor header.

Representation (*continued*):

TransArmor - VeriFone Edition (Encryption and Tokenization)—Initial Transaction—Request:

Format: TAPnnnnnnxyyyyy;yyyyyzzzz … *EDATA-MMYY%111NNNNNNNNNNNNNNNNNNNN

Where: TAPnnnnnnxyyyyy;yyyyyzzzz = the fixed length (25 bytes) TransArmor Header;

Followed by: … *EDATA-MMYY%111NNNNNNNNNNNNNNNNNNNN = the TA-VE encrypted data block, Expiration Date, and Settlement ID.

Content—TransArmor Header:

TAP = 3-byte TransArmor Indicator

Valid Value: TAP

nnnnnn = 6-byte Sequence Number of the transaction that matches the value in Element No. 63 (Sequence Number)

x = 1-byte EDATA (Element No. 126) Identifier that indicates the type of TA-VE support

Valid Value: 6 = TA-VE Support

yyyyy;yyyyy = 11-byte Key ID that includes a 5-byte Merchant Domain; followed by a semicolon(;); followed by a 5-byte Merchant Brand. These values are derived from the corresponding Merchant Profile.

zzzz = 4-byte Token Type ID

Valid Value: XXXX = Single use or MultiPay Token; 4-byte alphanumeric value assigned by First Data

… = Message data

* = Optional Data Area Field ID for Element No. 126 (EDATA)

EDATA = TA-VE encrypted data block (Track Data/PAN)

- = Optional Area Field ID for Expiration Date (Element No. 127)

MMYY = Expiration Date

% = Optional Area Field ID for Settlement ID (Element No. 134)

111 = Indicates the length (3 bytes) of the following Settlement ID.

NNNNNNNNNNNNNNNNNNNN = Settlement ID. It has a maximum length of 20 bytes.

TransArmor - VeriFone Edition (Encryption and Tokenization)—Initial Transaction—Response:

Format: 123456789012nn…nn

Where 123456789012nn…nn = The variable length (up to 25 alphanumeric bytes) retrieved Token.

Note: The last four bytes of the token are the same as the PAN's last four bytes.

Note: The Expiration Date is returned in the " – " Optional Data Area Field.

Note: Encrypted gift card PAN's are always returned in the clear.

Representation (*continued*):

TransArmor - VeriFone Edition (Encryption and Tokenization)—Follow-on Transaction—Request:

Format: TAPnnnnnnxyyyyy;yyyyyzzzz*EDATA-MMYY

Where: TAPnnnnnnxyyyyy;yyyyyzzzz = the fixed length (25 bytes) TransArmor Header;

Followed by *EDATA-MMYY = TA-VE encrypted data block and Expiration Date

Content—TransArmor Header:

TAP = 3-byte TransArmor Indicator

Valid Value: TAP

nnnnnn = 6-byte Sequence Number of the transaction that matches the value in Element No. 63 (Sequence Number)

x = 1-byte EDATA (Element No. 126) Identifier that indicates the type of TA-VE support

Valid Value: 0 = Token

yyyyy;yyyyy = zero-filled (00000;00000)

Note: A Key ID is not used.

zzzz = 4-byte Token Type ID

Valid Value: XXXX = Single use or MultiPay Token; 4-byte alphanumeric value assigned by First Data

TransArmor - VeriFone Edition (Encryption and Tokenization)—Follow-on Transaction—Response:

Format: 123456789012nn…nn

Where: "123456789012nn…nn" = The variable length (up to 25 bytes) retrieved Token.

Note: Encrypted gift card PAN's are always returned in the clear.

Processing Rules:

For non-TransArmor and TransArmor Token Only, the POS device maintains the card's Account Number until it receives a response from the host.

For TransArmor PKI Encryption and Tokenization, the POS device must not maintain the card's Account Number after the initial card swipe.

For all methods, if the Account Number is obtained from a Track 2 card reader, instead of being manually keyed, the Account Number and Card Discretionary Block Data should consist of all data.

For eParms enabled terminals, the terminal must include eParms data (variable length up to 300 characters). eParms includes information about the device as well as the status of the track/manually entered data. Once enabled, eParms data must be included with every transaction.

eParms data must follow the format preserving data. Format is preserved encrypted data and eParms are separated by the field separator "|".

Sample encrypted data from eParms enabled device is shown below:

3569994872982211=18122010231626951449|01010061250220150b284-109-

	108160d028410910800084102663d9b97017e527861032419f22370e8126d809000000286d302097c81
Valid Codes/Values:	See Appendix C. Valid Card Data Entries in the latest version of Host and Controller Interface Specifications.

Number:	33	**Name:**	Device ID
Character Type:	AN	**Length:**	11 bytes

R/O/C:	Optional
Representation:	Eleven-character number with no decimal places Left-aligned with trailing spaces
Purpose:	Identifies the device at which the transaction was created.
Processing Rules:	This data is assigned by each merchant. This data is unique for each merchant. It does not have to be unique among networks. It is required on all EFT transactions and messages. BUYPASS does not perform edits on this element. This data is required in a TransArmor PKI Key and Key ID Load Request and a TransArmor PKI Key and Key ID Load Response.
Valid Codes/Values:	Defined by the merchant.

Number:	40	**Name:**	Firmware Version
Character Type:	AN	**Length:**	8 bytes

R/O/C:	Required
Representation:	Eight alphanumeric characters
Purpose:	Identifies the current version of the device's firmware.
Processing Rules:	Not edited by BUYPASS, but is stored in the BUYPASS terminal database. This data is required in a TransArmor PKI Key and Key ID Load Request.
Valid Codes/Values:	

Number:	44	**Name:**	Hardware Version
Character Type:	AN	**Length:**	4 bytes

R/O/C:	Required
Representation:	Four alphanumeric characters
Purpose:	Identifies the current version of the device's hardware.
Processing Rules:	Not edited by BUYPASS, but is stored in the BUYPASS terminal database. This data is required in a TransArmor PKI Key and Key ID Load Request.
Valid Codes/Values:	

Number:	47	**Name:**	Manual Entry Flag
Character Type:	N	**Length:**	1 byte

R/O/C:	Required
Representation:	Single digit
Purpose:	Indicates whether PAN and expiration date have been entered using a keyboard, card reading device, bar code scanner, or radio frequency identification (RFID) device.
Processing Rules:	Set this element to 1 for transaction code 35 (resubmitted debit without PIN). This element must be populated correctly (code *2*) for RFID processing. The following processing rules apply to a TransArmor Authorization Request: • For encrypted Track1 or Track2 data, the value must be set to "0" for "swiped" data entry. • For encrypted PAN or tokenized data, the value must be set to "1" for "manual" data entry. • For encrypted PAN or tokenized data, the card's expiration date must be included in Data Element No. 127 (Expiration Date).

Valid Codes/Values:	Codes	Description
	0	PAN and expiration date entered using a card reading device or bar code scanner.
	1	PAN and expiration date entered using a keyboard.
	2	PAN and expiration date entered using a contactless reader.

Number: 53 Name: Optional Area Length

Character Type: N Maximum Length: 4 bytes

R/O/C:	Required
Representation:	Three or four numeric characters
Purpose:	Identifies the length, in bytes, of the following optional data area of the message.
Processing Rules:	If there is no optional data, this value is 000. This data is required in a TransArmor PKI Key and Key ID Load Request and a TransArmor PKI Key and Key ID Load Response. The maximum length is 3 bytes. This data is required in a TransArmor - VeriFone edition Response. The maximum length is 3 bytes. It follows Optional Data Area Field ID "%", and precedes transaction's Settlement ID (No. 134). In non-eWIC processing, this element has a maximum length of 3 numeric characters (999). In eWIC processing, this element has a maximum length of 4 numeric characters (9,999).
Valid Codes/Values:	Non-eWIC processing: 999 eWIC processing: 9,999

Number:	61	**Name:**	Record Type
Character Type:	A	**Length:**	3 bytes

R/O/C:	Required	
Representation:	Three uppercase letters	
Purpose:	Identifies the message being processed.	
Processing Rules:	This data is constant for each message. This element must appear as the first item in the record.	
Valid Codes/Values:	**Code**	**Message**
	SRQ	Synchronization Request
	SYN	Synchronization Response
	ARQ	Authorization Request
	ARP	Authorization Response
	HRQ	Health Request
	HRS	Health Response
	TRE	Totals Request
	TRP	Totals Response
	BRQ	BIN Load Request
	BIN	BIN Load Response
	STQ	TransArmor PKI Key and Key ID Load Request
	STP	TransArmor PKI Key and Key ID Load Response
	SSQ	Signing Key ID Load and Signed TransArmor Request
	SSP	Signing Key ID Load and Signed TransArmor Response

Number:	62	**Name:**	Response Code
Character Type:	N	**Length:**	2 bytes

R/O/C:	Required
Representation:	Two uppercase letters
Purpose:	Identifies additional information about the decision [Action Code (Element No. 1)] made by a card authorizer about the transaction.
Processing Rules:	In the case of a partial approval (approval with split tender), the card issuer approves the purchase by approving the purchase request up to the card's remaining balance—producing a zero balance on the card—and the store system prompts for the remaining amount due in order to complete the sale. For TransArmor non-Approved transaction, a Response Code is returned, and an Error Message displays in the Key ID and Key Data fields. **Note:** If a TransArmor Key Load (Signing/Signed/Unsigned) request is declined, the last element in the message will be Data Element 62 (Response Code).
Valid Codes/Values:	See Appendix D. Valid Response Codes in the latest version of the Host and Controller Interface Specifications.

Number:	63	**Name:**	Sequence Number
Character Type:	N	**Length:**	6 bytes

R/O/C:	Required
Representation:	Six-digit number with no decimal places Right-aligned and zero-filled
Purpose:	Identifies a transaction for the life of the transaction.
Processing Rules:	Assigned by the merchant's host/controller system when a transaction is received from the point-of-entry device. A unique sequence number must be generated for every transaction, except for the following transactions: • Time-out reversals (TOR) must have the same sequence number as the transaction being reversed. • Preauthorized completions must have the same sequence number as the original Authorization Only Request. It should be reset to *1* after the maximum value (*999999*) is reached. This data is required in a TransArmor PKI Key and Key ID Load Request and a TransArmor PKI Key and Key ID Load Response.
Valid Codes/Values:	1–999999

Number:	64	**Name:**	Software Version
Character Type:	AN	**Length:**	8 bytes

R/O/C:	Required
Representation:	Eight alphanumeric characters
Purpose:	Identifies the current version of the device's software.
Processing Rules:	Not edited by BUYPASS, but is stored in the BUYPASS terminal database. This data is required in a TransArmor PKI Key and Key ID Load Request.
Valid Codes/Values:	

Number:	80	**Name:**	Terminal Display
Character Type:	A	**Length:**	16 bytes

R/P/C:	Required
Representation:	Information displayed on the merchant's terminal
Purpose:	If a transaction is declined, an explanation is displayed.
Processing Rules:	BUYPASS requires that BUYPASS 16-byte response (Element No. 21) or one like it generated by the merchant's host/controller, be displayed, or printed on the journal/receipt at the store. This gives the consumer a clearer reason for a decline. If the merchant's host/controller generates its own response, it must correspond to the decline sent by BUYPASS. If the transaction is approved, the message "APPROVED" displays. **Note:** A BUYPASS-assigned decline code appears in positions 14 and 15 of this field. This code is useful when researching decline reasons with BUYPASS personnel. Required for both the TransArmor PKI Encryption and Tokenization and TransArmor Token Only Financial Transaction Response in which a Token has not been retrieved from the host.
Valid Codes/Values:	For TransArmor, the message indicates that BUYPASS has not been able to retrieve a token for the associated PAN for a TransArmor transaction.

Number:	81	**Name:**	Terminal Number
Character Type:	AN	**Length:**	11 bytes (except for TransArmor PKI Key ID and Key Load transaction, where the Terminal Number is 13 bytes)

R/O/C:	Required
Representation:	**All Transactions (except TransArmor PKI Key ID and Key Load)**: Eleven-digit value with the following components, left to right: • Two-digit State Code (Element No. 65) for terminal's physical location; • Six-digit BUYPASS Merchant ID (Element No. 4); and • Three-digit BUYPASS merchant terminal ID. **TransArmor PKI Key ID and Key Load transaction**: Thirteen-digit value with the following components, left to right: • Two-character Device Type (Required Value: ++); • Two-digit State Code (Element No. 65) for terminal's physical location; • Six-digit BUYPASS Merchant ID (Element No. 4); and Three-digit BUYPASS merchant terminal ID.
Purpose:	Provides unique identification of a merchant's store terminal for BUYPASS.
Processing Rules:	This number is assigned by BUYPASS. This data is required in a TransArmor PKI Key and Key ID Load Request and a TransArmor PKI Key and Key ID Load Response.
Valid Codes/Values:	For the two-digit State Code, use the ANSI® codes provided in Appendix E. Valid State Codes in the latest version of Host and Controller Interface Specifications.

Number:	82	**Name:**	Total Amount
Character Type:	N	**Length:**	10 bytes

R/O/C:	Required
Representation:	
Purpose:	Identifies the combined total amount for all approved transaction amount elements [Cash Amount (#19), Cash Benefit Amount (#21), Check Amount (#25), Debit Card Amount (#30), Discover Network Amount (#34), Food Stamp Amount (#41), MC/Visa Amount (#48), Proprietary Amount (#59), SVC Activation/Deactivation Amount (#67), SVC Purchase/Completion Amount (#69), SVC Recharge/Issue Amount (#71), SVC Replace Amount (#74), T/E Amount (#77), ECA/ TeleCheck® Amount (#113), and eWIC Amount (#125)].
Processing Rules:	ECA/ TeleCheck® service totals are returned for processing that includes a Version Number value of “700” or higher. eWIC totals are returned for processing that includes a Version Number value of “800” or higher. Any TransArmor processing (Version Number value of “900”) includes both ECA/ TeleCheck® service and eWIC totals.
Valid Codes/Values:	

Number:	83	**Name:**	Total Count
Character Type:	N	**Length:**	5 bytes

R/O/C:	Required
Representation:	
Purpose:	Identifies the combined total count for all approved transaction count elements [Cash Benefit Count (#23), Cash Count (#24), Check Count (#26), Debit Card Count (#31), Discover Network Count (#35), Food Stamp Count (#43), MC/Visa Count (#49), Proprietary Count (#60), SVC Activation/Deactivation Count (#68), SVC Purchase/Completion Count (#70), SVC Recharge/Issue Count (#72), SVC Replace Count (#75), T/E Count (#78), ECA/ TeleCheck® Count (#114), and eWIC Count (#124)].
Processing Rules:	ECA/ TeleCheck® service totals are returned for processing that includes a Version Number value of “700” or higher. eWIC totals are returned for processing that includes a Version Number value of “800” or higher. Any TransArmor processing (Version Number value of “900”) includes both ECA/ TeleCheck® service and eWIC totals.
Valid Codes/Values:	

Number:	86	**Name:**	Transaction Date
Character Type:	N	**Length:**	6 bytes

R/O/C:	Required
Representation:	YYMMDD
Purpose:	Identifies the date the transaction was created.
Processing Rules:	Merchant’s host/controller system date. This data is required in a TransArmor PKI Key and Key ID Load Request and a TransArmor PKI Key and Key ID Load Response.
Valid Codes/Values:	YY identifies the year (00–99) the transaction was created. MM identifies the month (01–12) the transaction was created. DD identifies the day (01–31) the transaction was created.

Number:	87	**Name:**	Transaction Time
Character Type:	N	**Length:**	6 bytes

R/O/C:	Required
Representation:	HHMMSS
Purpose:	Identifies the time the transaction was created.
Processing Rules:	Merchant's host/controller system time. This data is required in a TransArmor PKI Key and Key ID Load Request and a TransArmor PKI Key and Key ID Load Response.
Valid Codes/Values:	HH identifies the hour the transaction was created. MM identifies the minute the transaction was created. SS identifies the second the transaction was created.

Number:	113	**Name:**	ECA/ TeleCheck® Amount
Character Type:	N	**Length:**	10 bytes

R/O/C:	Required
Representation:	Variable length of up to 10 digits, with two implied decimal places
Purpose:	Identifies the total dollar amount of approved ECA/ TeleCheck® service check transactions.
Processing Rules:	ECA/ TeleCheck® service totals are returned for processing that includes a Version Number value of “700” or higher. Any TransArmor processing (Version Number value of “900”) includes ECA/ TeleCheck® service totals.
Valid Codes/Values:	0000000000–9999999999

Number:	114	**Name:**	ECA/ TeleCheck® Count
Character Type:	N	**Length:**	5 bytes

R/O/C:	Required
Representation:	Variable length of up to 5 digits
Purpose:	Identifies the total count of approved ECA/ TeleCheck® service check transactions.
Processing Rules:	ECA/ TeleCheck® service totals are returned for processing that includes a Version Number value of “700” or higher. Any TransArmor processing (Version Number value of “900”) includes ECA/ TeleCheck® service totals.
Valid Codes/Values:	00000–99999

Number:	124	**Name:**	eWIC Count
Character Type:	N	**Length:**	5 bytes

R/O/C:	Conditional
Representation:	Five digits
Purpose:	Identifies the total count of approved eWIC transactions.
Processing Rules:	eWIC totals are returned for processing that includes a Version Number value of “800” or higher. Any TransArmor processing (Version Number value of “900”) includes eWIC totals.
Valid Codes/Values:	00000–99999

Number:	125	**Name:**	eWIC Amount
Character Type:	N	**Length:**	10 bytes

R/O/C:	Conditional
Representation:	Ten digits with two assumed decimal places
Purpose:	Identifies the total dollar amount ($99,999,999.99) of approved eWIC transactions.
Processing Rules:	eWIC totals are returned for processing that includes a Version Number value of “800” or higher. Any TransArmor processing (Version Number value of “900”) includes eWIC totals.

Valid Codes/Values:	0000000000–9999999999

Number: 126 Name: EDATA

Optional Data Area Field ID: *

Character Type: ANS Length: 403 bytes

R/O/C:	Optional
Representation:	For PKI Encryption and Tokenization Processing, the first three bytes contain a fixed length 3-digit value that indicates the length of the following encrypted data block. For Token Only Processing, the first three bytes contain a fixed length 3-digit value that indicates the length of the following nonencrypted data block.
Purpose:	For PKI Encryption and Tokenization Processing, identifies the length and content of the encrypted data necessary to complete the transaction. For Token Only Processing, identifies the length and content of the nonencrypted data necessary to complete the transaction.
Processing Rules:	It is optional data; however, it must be present to support follow-on transactions for either PKI Encryption and Tokenization Processing or Token Only Processing. When present, it must be the first element in the Optional Data Area in Field No. 15.
Valid Codes/Values:	The element's maximum length is 403 bytes. This includes the fixed length 3-digit value—in the first 3 bytes—that indicates the length of the encrypted data block for PKI Encryption and Tokenization Processing or the nonencrypted data block for Token Only Processing.

Number:	127	**Name:**	Expiration Date
Optional Data Area Field ID:	- (hyphen)		
Character Type:	N	**Length:**	4 bytes

R/O/C:	Optional
Representation:	MMYY
Purpose:	Identifies the expiration date of the card.
Processing Rules:	It is conditional data; however, it must be present to support TransArmor when the Manual Entry Flag has a value of "1" for "manual" entry. This field will be returned on all TransArmor - VeriFone edition transactions using a value of "6" for the EDATA Identifier. For all TransArmor token initiated transactions, the Expiration Date must be sent in clear in this field. If sending a token in place of the PAN, then this element must be the first element in the Optional Data Area in Field No. 15.
Valid Codes/Values:	Any valid date.

Number:	128	**Name:**	Download Indicator
Optional Data Area Field ID:	+		
Character Type:	AN	**Length:**	1 byte

R/O/C:	Optional
Representation:	One digit
Purpose:	Indicates that the device needs to request a new TransArmor download because the current Key ID is due to or has expired.
Processing Rules:	It is optional data; however, it must be present to support TransArmor.
Valid Codes/Values:	A value of "8" indicates the need to perform a TransArmor download.

Number:	129	**Name**:	Key ID
Optional Data Area Field ID:	@		
Character Type:	AN	**Length:**	11 bytes

R/O/C:	Optional
Representation:	Eleven alphanumeric characters
Purpose:	Identifies the Key ID associated with the included encryption key.
Processing Rules:	It is optional data; however, it must be present to support TransArmor. Once requested and approved, this Key ID must be used in the Card Data (Element No. 18) for all subsequent TransArmor transactions from this device For a declined TransArmor transaction, an Error Message is returned in this field.
Valid Codes/Values:	Any valid TransArmor Key ID (including CA Key ID that is returned in response to a Signing Key request).

Number:	130	**Name:**	Key Data
Optional Data Area Field ID:	#		
Character Type:	AN	**Length:**	400 bytes

R/O/C:	Optional
Representation:	Variable length of 3 alphanumeric characters
Purpose:	Identifies the new encryption Key and the Key ID (Element No. 129) associated with it or the Error Message.
Processing Rules:	For an approved TransArmor transaction, the maximum length is 400 bytes. For a declined TransArmor transaction, a message is returned in this field.
Valid Codes/Values:	Any valid key (including Signing Key and Signed Key that is returned in response to a Signing Key request).

Number:	134	**Name:**	Settlement ID
Optional Data Area Field ID:	% (Percent Sign)		
Character Type:	ANS	**Length:**	20 bytes

R/O/C:	Optional
Representation:	Variable maximum length of up to 20 bytes
Purpose:	Identifies the transaction's Settlement ID in a TransArmor - VeriFone edition transaction.
Processing Rules:	The Optional Data Area Field ID is always a Percent Sign (%). This data is required in a TransArmor - VeriFone edition transaction.
Valid Codes/Values:	Any valid Settlement ID