Triton Terminal
Communications Protocol
And Message Format Specification

Triton

A DOVER COMPANY

PRELIMINARY

VERSION TSCD5.22

July 19, 2004

Limitations

Table of Contents

VERSION SUMMARY

Version	Date	Summary of Changes
TSCD5.22 †	07/19/04	Updated maximum communications buffer size.
TSCD5.21 †	07/12/04	Updated Appendix G – New information about 'ud' FID, tag 8A, and tag 89.
TSCD5.20 †	06/30/04	Updated "Limitations" statement
TSCD5.19 †	04/08/04	Updated 'za' FID to include a more accurate explanation of encrypting sender IDs.
TSCD5.18 †	03/30/04	Clarified the downloading of the store, marketing, welcome, and exit messages using the 'd' miscellaneous field.
TSCD5.17 †	03/11/04	Updated Appendix G – New information about PAN (5A) tag, typographic corrections.
TSCD5.16 †	2/27/04	Updated Appendix G – New information on the Transaction Sequence Counter tag (9F41).
TSCD5.15 †	2/16/04	Updated host total response to include spaces for the number of transactions and settlement amount fields.
TSCD5.14 †	2/13/04	Added FID 'ui' – Motorized card reader commands.
TSCD5.13 †	11/14/03	Updated Reversal Reason Codes (FID 'n'). Updated 'xq' FID to include a disable all command.
TSCD5.12 †	11/06/03	Updated Valid Misc. FID table. Updated lists of EMV data elements in requests and reversals.
TSCD5.11 †	10/31/03	Updated Appendix G with corrections, additions, and clarifications.
TSCD5.10 †	10/23/03	Updated Appendix G with corrections.
TSCD5.9 †	10/01/03	Updated Appendix G with information about issuer script results.
TSCD5.8 †	9/29/03	Added FID 'uh' – Encoded EMV untagged-data block Added description of this block to appendix G.
TSCD5.7 †	9/26/03	Updated the description of the 'za' FID
TSCD5.6 †	9/22/03	Fixed error in Appendix H – Top Up
TSCD5.5 †	9/16/03	Updated the MAC enable/disable field - '/0' is not allowed in Configuration Download Response Messages. Updated Appendix B to include Triple-DES MACing flowchart for clarification that Triple-DES should only be done for the last round of the algorithm. Updated to ANSI Standard X9.19 format for MAC. Added the Triple-DES MAC Algorithm is defined in ISO/IEC 9797-1.
TSCD5.4 †	8/28/03	Added FID 'ug' – Host Transaction Trace Number
TSCD5.3 †	8/6/03	Updated Appendix E – Changed description to "Encryption Key Sets". Updated Appendix B– Added Triple-DES encryption option for MAC. Updated FID 'm' – MAC working key left block Added FID '}' – MAC working key right block Added FID 'ue' – Data working key left block Added FID 'uf' – Data working key right block
TSCD5.2 †	7/23/03	Added authorization code 035 – Second Invalid PIN
TSCD5.1 †	6/26/03	Added Appendix H – Top Up
TSCD5.0 †	6/16/03	Added appendix G for EMV data elements. Added maximum message length to 2048 for terminal's that support large message buffers. Added authorization codes 033 and 034 Added FID 'ud' – Encoded EMV data block
TSCD4.4 †	6/12/03	Updated Valid Miscellaneous Field ID Table to include 'va' in host totals request message. Added reversal reason '06' – VAS Challenge/Response Error. Fixed the protocol description for a correctable request response.
TSCD4.3 †	5/27/03	Added FID 'xu' – Service provider ID. Added FID 'xv' – . Service provider transaction totals and amounts.

		Modified FID 'xg' Added Authorization codes 028 – 032 for pre-pay transactions.
TSCD4.2 †	5/5/03	Removed trademark references
TSCD4.1 †	4/29/03	Removed 'xt' FID from Host Totals response message.
TSCD4.0 †	4/16/03	Added PC Based Products family to Product Code table. Updated description of software version number fields in status monitoring for PC Based products. Added new 9600 family prefix to Product Code table.
TSCD3.9 †	4/11/03	Modified FID 'xr' Changed FIX 'zc' to numeric only. Changed Transaction Code '52' to long distance recharge only. Added Transaction Code '53' – Purchase new long distance calling plans. Added FID 'zn' - PAN used for Western Union Receive transaction request.
TSCD3.8 †	2/11/03	Changed Easy Pay Bill Payment to Bill Payment to make it more generic.
TSCD3.7 †	2/10/03	Added FID 'yf' – Easy Pay Bill Payment amounts and totals.
TSCD3.6 †	1/27/03	Modified Amount 1 field of the Transaction Response Message to indicate the amount to dispense for transaction codes "48" and "49" only.
TSCD3.5 †	1/23/03	Added © Delaware Capital Formation, Inc. to title page changed check cashing PIN to 3 to 6 characters in length. updated Valid Miscellaneous Field ID Table.
	1/13/03	Added FID-group 'u' for general purpose FIDs. Added FID 'ua' – Date synchronization with host. Updated description of 't' FID to indicate it may be used with the 'ua' FID to update both the time and date of the terminal. Added FID 'ub' – ANSI 16-bit CRC used for any message type. Added FID 'u~', 'u{' , 'um' , 'un' , 'uo' , 'up' , 'u[' – Encrypted Working Keys. Added Appendix E – Multiple Service Encryption Keys Added Appendix F – ANSI 16-bit CRC Added authorization code '027' – CRC error Added max message length cannot exceed 512 bytes.
TSCD3.4 †	12/20/02	Added to FID-group 'x': Added FID 'xt' –Sales tax rate for wireless or long distance transactions.

TSCD3.3 †	12/02/02	Added Transaction Code '52'.
		Updated FID 'xd' and FID '!' – max amount cannot exceed "0032767"
		Added to FID-group 'x':
		     Added FID 'xq' – Service provider name and fast cash amounts for wireless transactions.
		     Added FID 'xr' - Long distance calling plans.
		     Added FID 'xs' - Long distance amounts and totals.
		Added to FID-group 'y':
		     Added FID 'ye' – Check cashing amounts and totals.
		Added to FID-group 'z':
		     Added FID 'zk' – Funds-send amounts and totals.
		     Added FID 'zm' – Funds-receive amounts and totals.
		
		Added Authorization code '025' for Western Union Sender data Error
		Added Authorization code '026' for Western Union Receiver data Error

TSCD3.2 †	8/27/02	Updated FID 'xb' – Added user's mobile phone number for prepaid offline or online transactions when used in a transaction request message. Added FID 'vd' – VAS Challenge/Response field. Added 'KX' to product code table for EPROM versions for model 9100 family.
TSCD3.1 †	8/16/02	Added FID-group 'v' for generic Value Added Service fields. Added FID 'va' – Alternate Terminal ID for Value Added Service. Added FID 'vb' – Zip code of Terminal for Value Added Service. Added FID 'vc' – Loyalty card information for Value Added Service. Updated FID-group 'y' to include Check Cashing fields. Added FID 'yc' – Check cashing Authorization code.

		Added FID 'yd' – Check cashing PIN (either encrypted or not encrypted)
		Added transaction code "48" - Check Cashing Withdrawal
		Modified Amount 1 field of the Transaction Response Message to indicate the amount to dispense for transaction code "48" only.
		Updated the format of the Valid Miscellaneous FID Table.
TSCD3.0 †	6/26/02	Added FID-group 'y' for Prepaid Telephone, Easy Pay Bill payment, and Prepaid Electricity Added FID 'ya' - Easy pay account or electricity meter number Added FID 'yb' - Receiver name for easy pay bill payment or prepaid electricity transaction Revised Appendix C: Added extended transaction code "04" – Prepaid Telephone Added extended transaction code "05" – Easy Pay Bill Payment Added extended transaction code "06" – Prepaid Electricity Added to FID-group 'x': Added FID 'xn' - Actual amount debited form the customer's account for prepaid online transactions. Added FID 'xp' - Voucher PIN number for prepaid online transactions.
	6/13/02	Added 9100 and 9800 to Product Code tables Corrected descriptions for FID-group 'x' Updated for Funds Transactions Requirements Added transactions type "46" - Funds Send from Checking Added transactions type "47" - Funds Send from Savings Added transactions type "48" - Funds Receive Added FID 'za' – Encrypted Sender ID for Funds. Added FID 'zb' – Preferred Customer ID for Funds. Added FID 'zc' – Confirmation ID for Funds. Added FID 'zd' – State tax value for Funds. Added FID 'ze' – Money Transfer Control number for Funds. Added FID 'zf" – Funds enable or disable. Added FID 'zg' – Western Union telephone number for Funds. Added FID 'zh' – Maximum request amount for a Funds transaction. Added FID 'zi' – Smallest denomination multiple-amount for a Funds transaction. Added FID 'zj' – Funds convenience fee amount.
TSCD2.9 †	2/4/02	Added "ts" to the Terminal Identifier field for Triton Scrip
	1/30/02	Added FID '[' – ASCII Char 5Bh – Terminal is Triple-DES capable Revised Appendix D
	1/10/02	Changed to '1=reserved' for the Encryption Mode Flag of the Information Header in the Request Messages which support the Information Header (or Comms Header). Added Model 9700 to Product Code tables. Clarified Status Monitoring Field. The first character of the Status Monitoring Field will always be a capital letter (A - Z). Clarified Terminal Totals Fields. The first character, and all characters, of the Terminal Totals Fields will always be numeric (0 – 9). Added Appendix D – Triple-DES Encryption of the PIN Block Added '2=Triple DES encryption of the PIN block' to the Encryption Mode Flag of the Information Header in the Request Messages which support the Information Header (or Comms Header). Added FID '{' – ASCII Char 7Bh – Triple-DES Encrypted PIN-Key 2 ($K2$) Added transactions type "44" - Non-Financial prepaid online transaction (POS type transaction) Added FID-group 'x' for prepaid offline and/or online transactions. Added FID 'xa' – Telco product serial number for online transactions. Added FID 'xb' – activation phone number for prepaid offline or online transactions. Added FID 'xc' – Taxes 1 – (GST/HST/PST taxes for offline transactions) or general taxes for offline transactions. Added FID 'xd' – Taxes 2 - general taxes for online transactions

		Added FID 'xe' - Host Total amounts for prepaid online transactions. Added FID 'xf' – Contact phone number for prepaid offline or online transactions. Added FID 'xg' – Carrier name for prepaid offline or online transactions. Added FID 'xh' – Expiration date for online transactions. Added FID 'xi' – Secret number of prepaid offline or online transactions.
TSCD2.7k†	6/15/01	Changed Miscellaneous FID 'o' to fixed length - 12 Numeric total characters.
TSCD2.7j†	5/23/01	Updated Appendix C – Extended Transaction Code Table to include eight new transaction types. The types now include eight for Bank Transaction Types, and eight for Brokerage Transaction Types.
TSCD2.7i	5/14/01	Added transactions type "99" - Extended Transaction Code. Added Miscellaneous FID 'l' (ASCII Char 6Ch) for Extended Transaction Codes. Added Appendix C – Extended Transaction Code Table Changed text of checking, savings, and credit card account's to include 'primary' and 'secondary'.
	03/30/01	Added transaction type, "43" - Quasicash CREDIT ADVANCE Added Miscellaneous FID 'o' – ASCII Char – 6Fh for Quasicash CREDIT total amounts. Added note about the Quasicash authorization number in the Transaction Response Message. The authorization code will be alphanumeric for Quasicash transactions and space filled to the left if less than 8 characters.
TSCD2.7h	11/20/00	Added Miscellaneous Field ID 'n' to indicate reason for a reversal.
TSCD2.7	9/11/00	Absence of 'k' field implies unknown Issuer Fee/Credit.
	8/30/00	Clarified 'k' field. Absence implies zero Issuer Fee/Credit. 'k' allowed in reversal, as well as, the transaction reply.
	8/28/00	Added Miscellaneous Field ID 'k' for issuer fee/credit.
	8/18/00	Modified Amount 2 fields in Transaction Request and Transaction Response to allow negative amounts.
	2/8/00	Clarified 'g' and 'i' FIDs to indicate that the fields are not mandatory if track 3 is supported by the card reader. If the fields are used in the message AND the track 3 data is faulty, the field only contains the FID code. Added N and P program designators in Product Code Table for Program / Table Version Numbers. Added N in Product Code Table for EPROM Version Numbers.
	1/21/00	Added Miscellaneous Field ID 'g' for Track 3 data. Added FID 'g' to Valid Miscellaneous FID Table in Request and Reversal messages. This FID is only used with terminals configured with track 2-3 readers. Added Miscellaneous Field ID 'i' for PAN from track 3. Added FID 'i' to Valid Miscellaneous FID Table in Request and Reversal messages. This FID is only used with terminals configured with track 2-3 readers.
	5/10/99	Corrected typo of sentinel (misspelled as sentinal). Removed duplicate entry in Miscellaneous FID Table for 't'. Added support for multiple Miscellaneous Fields in all packet types. Added Miscellaneous Field ID '&' to support return of Account Number in Transaction Response. Added ability to use 'e' Miscellaneous Field ID to support return of 12 digit settlement amount in Host Totals Response. Added Miscellaneous Field ID '#' to support sending 12 digit sequence number to host in Transaction Request and Reversal Request. Added new Transaction Request Code '01' for PIN Change. Added Miscellaneous Field ID '@' to support sending PIN Change PIN Block. Added Authorization Code '222' for PIN Change failed. Added Valid Miscellaneous FID Table

		Added new Authorization Codes to allow for more complete coverage of possible error conditions.
TSCD2.6	2/16/99	Modified MAC Protocol Addendum to reflect all messages that include a MAC.
		Added Message Protocol with MAC enabled diagram to the end of this document.
	12/22/98	Added Appendix B (Triton MAC protocol).
		Deleted FID 'a', authentication field, replaced by MAC fields
		Added FID '/', '^', and 'm' to support MAC protocol.
		Added FID 'w' for Maximum withdraw amount
		Added FID 'h' for Heartbeat interval
		Added FID 'c' for automatic day close time setting
		Added FID 't' for time synchronization with host
		Added FID 'd' for download of programmable messages
		Added support for more than two FID fields in Configuration Table Download Response Message
		Changed FID '~' in Configuration Table Download Response Message from optional to required
		Added optional field group to Host Totals Download Request top report terminal totals to host
		Added new value of 'X – Not installed' in subfields Alarm, Chest door open; Alarm, Top door open; Journal printer, paper status; Journal printer, ribbon status of Status Monitoring field
		Added , '<Spaces> - Not supported' to Electronics system subfield in Status Monitoring field
		Removed 'Transaction' from Miscellaneous Field ID Descriptions table. New format of this table indicates which response messages can contain the individual FIDs. Changed wording at end of this table to indicate that FIDs may appear in any miscellaneous field, where appropriate.
TSCD2.5	3/19/98	Added Field ID code for authentication field in response message (FID 'a').
		Incorporated dial-up protocol specification into this document.
		Added table of contents and page numbers to document.
		Added Appendix A (ANSI X.9.8 excerpts)
TSCD2.4	11/21/97	The status monitoring field is terminated by a field separator, but prior to this release, it was not clear that this FS was part of the status monitoring field itself. This version specifically states that the trailing FS is part of the optional field and is NOT sent if the field is not enabled.
		Document reformatted and now produced using Microsoft Word 97.
		Added model 9600 to all references of product. Model 9500 and 9600 and completely software compatible.
		Added product description tables to explain coding of firmware version numbers in status field.
		Added transaction 61, 62, 65, 71, 72, 75, 81, 82, 85, 91, 92, and 95. All of these transactions use a miscellaneous field for

		the amount of the withdrawal, transfer or balance inquiry. These codes were added to allow amounts to be used that are greater that 8 characters in length.
		The Miscellaneous fields in the Transaction Response message were listed as F for fixed length but described as Variable Alphanumeric for the length/type description. They have been clarified to be variable length to be consistent.
		Changed FID 'b' field description from ledger balance to available balance.
		Added Field ID code type 'e' to represent extended length amounts. When used, it overrides the amount 1 field in the request or the response message. This FID may appear in requests and responses.
		The reference to implied decimal points in amount fields has been changed to indicate that all amount fields are formatted in the smallest unit of currency possible for the installed country. For the US, this is pennies. This is not a change in the way the field is represented, only a change in how it is described. The implication of decimal places can be assumed based on the local requirements.
		Changed Miscellaneous field 1 and 2 in transaction request message from fixed length to variable length.
		Added capability for more than two miscellaneous field to be returned in transaction response message
TSCD2.3B	9/5/97	Added field separator between amount 3 and status field in reversal request message. This is not a spec. Change, but correction of an omission.
TSCD2.3A	6/27/97	Changed description of 'p' printing field to include error receipts, as well as responses.
TSCD2.3	5/18/97	Added Field ID code for receipt text (FID 'p') transaction response message and host totals response message.
		Changed specified length of Miscellaneous fields from fixed at 20 to variable to accommodate FID p.
		Added support at 2400 baud.
TSCD2.2	2/11/97	Added status monitoring at the end of all messages. This data is switchable at the terminal to enable or disable it being sent. If enabled, it is sent at the end of every message sent to the host.
		Added Field ID code for additional balances (FID 'b')
	3/18/97	Added Field ID code for surcharge amount (FID !). This FID was already included in the Configuration download Response message. It is now supported in any response Misc. field.
TSCD2.1	1/24/97	Made Communications Identifier, Terminal Identifier, Software Version No. and Information Header fields optional in all request messages to the host.
		Noted that corresponding information header fields in the response messages are optional and only sent when the request messages contain the optional fields.
		Specified the first character of the Information header to be the DES Indicator flag. The last seven characters are still undefined.
TSCD2.0	6/10/96	Formal release of Version 2 Specification.
		This specification is an upgrade from the first generation. It adds several features, which include but are not limited to:
		Deleted version number and date from each table in document.
		Added support for communications key download in transaction response messages.
		Added transaction codes 41, 42, and 45
		Added Communications Identifier, Terminal Identifier, Software Version No. and Information Header fields in each request message to host.
		Added version summary page.

MODEM COMMUNICATION PARAMETERS

The modem communications parameters are:

- 300, 1200, or 2400 bps
- 7 data bits
- even parity
- 1 stop bit
- Asynchronous

The modem complies with Bell 212A/103 and CCITT V.22 standards.

The LRC (Longitudinal Redundancy Check) is always the last character of the message. This character is the Exclusive OR of all characters in the message, starting with the first character after the STX, through and including the ETX.

The maximum length of a typical transmitted message cannot exceed 512 bytes including the STX, ETX, and the LRC.

For terminal software versions that support large message buffers the maximum length of a transmitted message cannot exceed 2000 bytes including the STX, ETX, and the LRC. For protocol problems "Terminal ACK Not Received By Host" and "Terminal Does Not Acknowledge Response From Host" the 3-second timeout counter should start **after** the LRC is transmitted from the MODEM.

[†]**Preliminary**.

Control Character Table	
STX	02h
ETX	03h
EOT	04h
ENQ	05h
ACK	06h
NAK	15h
FS	1Ch

Transaction Request Message

Field Name	Length/Type	Fixed/Var.	Reqd	Opt.	Description
STX	1 ASCII Char.	F	X		Start of text character
Communications Identifier	8 ASCII Char.	F		X*	A text string used to identify the 'owner' of the message to a communications service provider. Default string is "XXXXXX^^". ^ characters are spaces and are required. 'X' characters represent identification string for processor.
Terminal Identifier	2 ASCII Char.	F		X*	Lower case 't' and lower case 'd' or 's', indicating to host the type of terminal
Software Version No.	2 ASCII Char.	F		X*	Two digit Base 36 number representing the version of software installed on the terminal. Starts at '00'
Encryption Mode Flag	1 ASCII Char.	F		X*	0 = Single DES encryption of PIN block. 1 = Reserved. 2 = Triple DES encryption of PIN block.
Information Header	7 ASCII Char.	F		X*	Seven byte field, unused as of this release. Must be space filled.
FS	1 ASCII Char.	F		X*	Field separator
Terminal ID	15 Alphanumeric	F	X		Terminal ID. Assigned by processor. Left justified, space filled to the right.
FS	1 ASCII Char.	F	X		Field separator
Transaction Code	2 Alphanumeric	F	X		Code indicating type of transaction being done. See Transaction Codes table.
FS	1 ASCII Char.	F	X		Field separator
Sequence Number	4 Numeric	F	X****		Consecutive number from 1-9999 set by terminal. Rolls over at 9999. Tags a transaction as a unique event. Each subsequent transaction is guaranteed to have different sequence number.
FS	1 ASCII Char.	F	X		Field separator
Track 2	37 Numeric	V	X		Complete track 2 data, excluding the Start Sentinel, End Sentinel, and LRC
FS	1 ASCII Char.	F	X		Field separator
Amount 1	8 Numeric	F	X		Withdraw or transfer amount. Zero filled to the left. Represents the amount in the smallest possible unit of currency.
FS	1 ASCII Char.	F	X		Field separator
Amount 2	8 Numeric	F	X		Surcharge amount as set by terminal. Zero filled to the left. Represents the amount in the smallest possible unit of currency. An ASCII minus sign (e.g. "-0000100") in the first position represents a credit.
FS	1 ASCII Char.	F	X		Field separator
PIN Block	16 Alphanumeric	F	X		ANSI standard encrypted PIN block. (See Appendix A)
FS	1 ASCII Char.	F	X		Field separator
Miscellaneous 1	Variable Alphanumeric	V		X	Can contain user defined information.
FS	1 ASCII Char.	F	X		Field separator

Transaction Request Message

Miscellaneous 2	Variable Alphanumeric	V		X	Can contain user defined information.
FS	1 ASCII Char.	F	X		Field separator
Status Monitoring Field	XX ASCII Chars.	F		X**	Contains status information about terminal. Refer to table for full field format later in this document.
FS	1 ASCII Char.	F		X**	Field separator
Miscellaneous X	Variable Alphanumeric	V		X***	Can contain user defined information.
FS	1 ASCII Char.	F		X***	Field separator
ETX	1 ASCII Char	F	X		End of text Character
LRC	1 Hexadecimal Char	F	X		Longitudinal Redundancy Check. Exclusive OR (XOR) of all characters starting with the first character after the STX, through and including the ETX.

* These fields are optional only as a group. The terminal contains a management function to enable or disable the sending of this group of fields. This group was added in version 2.0, and was made optional in version 2.1 to allow compatibility with older host drivers. If the field group is not enabled on the terminal, these fields will not be sent. If they are not sent, the corresponding fields in the response messages should not be returned.

** This field (Status Monitoring Field) is optional and can be enabled or disabled at the terminal level. If enabled, it is sent on *ALL* messages up to the host. No response is expected to the sending of this information. The first character of the Status Monitoring Field will always be a capital letter (A - Z).

*** As of version 2.7, more than two miscellaneous fields are allowed for. Each field must include a valid FID code and data and be terminated by a field separator. See Valid Misc. FID table.

**** As of version 2.7, If 12 digit sequence number is being sent as a miscellaneous field, this field should be padded with 4 spaces.

Transaction Response Message

Field Name	Length/Type	Fixed/ Var.	Reqd	Opt.	Description
STX	1 ASCII Char.	F	X		Start of text character
Information Header	12 ASCII Char.	F		X*	Not used as of this release, must be space filled
FS	1 ASCII Char.	F		X*	Field separator
Multi-Block Indicator	1 Numeric	F	X		0 = single block response 1= another block will follow this block. Last block must always be 0.
FS	1 ASCII Char.	F	X		Field separator
Terminal ID	15 Alphanumeric	F	X		Copied from request message.
FS	1 ASCII Char.	F	X		Field separator
Transaction Code	2 Alphanumeric	F	X		Copied from request message.
FS	1 ASCII Char.	F	X		Field separator
Sequence Number	4 Numeric	F	X		Copied from request message.
FS	1 ASCII Char.	F	X		Field separator
Response Code	3 Numeric	F	X		Result of request. Approved = 000. Non-0000 = declined. See Authorization Codes for list of decline codes.
FS	1 ASCII Char.	F	X		Field separator
Authorization Num.	8 Numeric	F	X		Authorization number generated by the processor for the transaction. Right justified, zero filled to the left if not 8 characters. (note: This field is alphanumeric for Quasicash type transaction responses, Zero(030h) or space(020h) filled to the left if less than 8 characters.)
FS	1 ASCII Char.	F	X		Field separator
Transaction Date	6 Numeric	F	X		Date of transaction in MMDDYY format. Set by processor.
FS	1 ASCII Char.	F	X		Field separator
Transaction Time	6 Numeric	F	X		Time of the transaction in HHMMSS format. Set by processor.
FS	1 ASCII Char.	F	X		Field separator
Business Date	6 Numeric	F	X		Business date of the transaction in MMDDYY format. Set by processor.
FS	1 ASCII Char.	F	X		Field separator
Amount 1	8 Numeric	F	X		**Balance amount**. Zero filled to the left, right justified. If space filled, no balance available (for W/D transactions) Represents the amount in the smallest possible unit of currency. **Amount to dispense**. Use for transaction codes: "48" – Check Cashing Withdrawal. "49" – Receive Money.
FS	1 ASCII Char.	F	X		Field separator

Transaction Response Message						
Amount 2	8 Numeric	F	X		Amount of actual surcharge Zero filled to the left, right justified. Represents the amount in the smallest possible unit of currency. An ASCII minus sign (e.g. "-0000100") in the first position represents a credit.	
FS	1 ASCII Char.	F	X		Field separator	
Miscellaneous 1	Variable Alphanumeric	V		X	Miscellaneous data. Refer to Miscellaneous Field ID codes for possible uses for this field.	
FS	1 ASCII Char.	F	X		Field separator	
Miscellaneous 2	Variable Alphanumeric	V		X	Miscellaneous data. Refer to Miscellaneous Field ID codes for possible uses for this field.	
FS	1 ASCII Char.	F	X		Field separator.	
Miscellaneous X**	Variable Alphanumeric	V		X**	Miscellaneous data. Refer to Miscellaneous Field ID codes for possible uses for this field.	
FS**	1 ASCII Char.	F		X**	Field separator.	
ETX	1 ASCII Char	F	X		End of text Character	
LRC	1 Hexadecimal Char	F	X		Longitudinal Redundancy Check. Exclusive OR (XOR) of all characters starting with the first character after the STX, through and including the ETX.	

* These fields are optional only as a group. They should only be included in responses to requests that contain the corresponding optional fields. Refer to the request message table for further information.

If the FID 'p' is returned in either MISC. 1 or MISC. 2, the data will be printed on all approved and declined transactions.

** As of version 2.4, more than two miscellaneous fields are allowed for. Each field must include a valid FID code and data and be terminated by a field separator. See Valid Misc. FID table.

Configuration Table Download Request Message

Field Name	Length/Type	Fixed/ Var.	Reqd	Opt.	Description
STX	1 ASCII Char.	F	X		Start of text character
Communications Identifier	8 ASCII Char.	F		X*	A text string used to identify the 'owner' of the message to a communications service provider. Default string is "XXXXXX^^". ^ characters are spaces and are required. 'X' characters represent identification string for processor.
Terminal Identifier	2 ASCII Char.	F		X*	Lower case 't' and lower case 'd' or 's', indicating to host the type of terminal.
Software Version No.	2 ASCII Char.	F		X*	Two digit Base 36 number representing the version of software installed on the terminal. Starts at '00'
Encryption Mode Flag	1 ASCII Char.	F		X*	0 = Single DES encryption of PIN block. 1 = Reserved. 2 = Triple DES encryption of PIN block.
Information Header	7 ASCII Char.	F		X*	Seven byte field, unused as of this release. Must be space filled.
FS	1 ASCII Char.	F		X*	Field separator
Terminal ID	15 Alphanumeric	F	X		Terminal ID. Assigned by processor. Left justified, space filled to the right.
FS	1 ASCII Char.	F	X		Field separator
Transaction Code	2 Alphanumeric	F	X		Code indicating type of transaction being done. Transaction code = 60 for Configuration Table Download.
FS	1 ASCII Char.	F	X		Field separator
Status Monitoring Field	XX ASCII Chars.	F		X**	Contains status information about terminal. Refer to table for full field format later in this document.
FS	1 ASCII Char.	F		X**	Field separator
Miscellaneous X	Variable Alphanumeric	V		X***	Can contain user defined information.
FS	1 ASCII Char.	F		X***	Field separator
ETX	1 ASCII Char	F	X		End of text Character
LRC	1 Hexadecimal Char	F	X		Longitudinal Redundancy Check. Exclusive OR (XOR) of all characters starting with the first character after the STX, through and including the ETX.

* These fields are optional only as a group. The terminal contains a management function to enable or disable the sending of this group of fields. This group was added in version 2.0, and was made optional in version 2.1 to allow compatibility with older host drivers. If the field group is not enabled on the terminal, these fields will not be sent. If they are not sent, the corresponding fields in the response messages should not be returned.

** This field (Status Monitoring Field) is optional and can be enabled or disabled at the terminal level. If enabled, it is sent on *ALL* messages up to the host. No response is expected to the sending of this information. The first character of the Status Monitoring Field will always be a capital letter (A - Z).

*** As of version 2.7, multiple Miscellaneous fields are allowed for. Each field must include a valid FID code and data and be terminated by a field separator. See Valid Misc. FID table.

Configuration Table Download Response Message

Field Name	Length/Type	Fixed/ Var.	Reqd	Opt.	Description
STX	1 ASCII Char.	F	X		Start of text character
Information Header	12 ASCII Char.	F		X*	Not used as of this release, must be space filled
FS	1 ASCII Char.	F		X*	Field separator
Terminal ID	15 Alphanumeric	F	X		Terminal ID. Assigned by processor. Left justified, space filled to the right.
FS	1 ASCII Char.	F	X		Field separator
Transaction Code	2 Alphanumeric	F	X		Code indicating type of transaction being done. Transaction code = 60 for Configuration Table Download.
FS	1 ASCII Char.	F	X		Field separator
Field ID Code	'~'	F	X		The '~' character indicates the field is the Pin Working Key 1.
Encrypted PIN Key	16 Alphanumeric	F	X		PIN Working Key 1. This key is encrypted by the PIN Master Key before being transmitted to the terminal.
FS	1 ASCII Char.	F	X		Field separator
Field ID Code	'!'	F		X	The '!' character indicates the field is the maximum allowed surcharge amount.
Surcharge amount	8 Numeric	F		X	The surcharge amount that the terminal will display to the customer and charge for the transaction(Note: actual surcharge may be less than this amount). Right justified, zero filled to the left. Represents the amount in the smallest possible unit of currency.
FS	1 ASCII Char.	F	X		Field separator
Miscellaneous X**	Variable Alphanumeric	V		X	Miscellaneous data. Refer to Miscellaneous Field ID codes for possible uses for this field.
FS	1 ASCII Char.	F		X	Field separator, needed only if Miscellaneous field X is present.
ETX	1 ASCII Char	F	X		End of text Character
LRC	1 Hexadecimal Char	F	X		Longitudinal Redundancy Check. Exclusive OR (XOR) of all characters starting with the first character after the STX, through and including the ETX.

NOTE:
* These fields are optional only as a group. They should only be included in responses to requests that contain the corresponding optional fields. Refer to the request message table for father information.

** As of version 2.4, more than two miscellaneous fields are allowed for. Each field must include a valid FID code and data and be terminated by a field separator. See Valid Misc. FID table.

Fields will be added to the end of this message as needed. Each field will have a Field ID Code associated with it. Fields do not have to be in any order, and are not required in each message. The terminal will use the ID code to process all fields sent.

Host Totals Download Request Message

Field Name	Length/Type	Fixed/Var.	Reqd	Opt.	Description
STX	1 ASCII Char.	F	X		Start of text character
Communications Identifier	8 ASCII Char.	F		X*	A text string used to identify the 'owner' of the message to a communications service provider. Default string is "XXXXXX^^". ^ characters are spaces and are required. 'X' characters represent identification string for processor.
Terminal Identifier	2 ASCII Char.	F		X*	Lower case 't' and lower case 'd' or 's', indicating to host the type of terminal
Software Version No.	2 ASCII Char.	F		X*	Two digit Base 36 number representing the version of software installed on the terminal. Starts at '00'
Encryption Mode Flag	1 ASCII Char.	F		X*	0 = Single DES encryption of PIN block. 1 = Reserved. 2 = Triple DES encryption of PIN block.
Information Header	7 ASCII Char.	F		X*	Seven byte field, unused as of this release. Must be space filled.
FS	1 ASCII Char.	F		X*	Field separator
Terminal ID	15 Alphanumeric	F	X		Terminal ID. Assigned by processor. Left justified, space filled to the right.
FS	1 ASCII Char.	F	X		Field separator
Transaction Code	2 Alphanumeric	F	X		Code indicating type of transaction being done. See Transaction Codes table. For Host totals, code is either 50 or 51.
FS	1 ASCII Char.	F	X		Field separator
Status Monitoring Field	XX ASCII Chars.	F		X**	Contains status information about terminal. Refer to table for full field format later in this document.
FS	1 ASCII Char.	F		X**	Field separator
No. of Withdrawals (Terminal)	4 Numeric	F		X***	Total number of withdrawals since the last request for totals. Zero filled to the left.
No. of Inquiries (Terminal)	4 Numeric	F		X***	Total number of inquiries since the last request for totals. Zero filled to the left.
No. of Transfers (Terminal)	4 Numeric	F		X***	Total number of transfers since the last request for totals. Zero filled to the left.
Settlement (Terminal)	12 Numeric	F		X***	Total amount of all withdrawals. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.
FS	1 ASCII Char.	F		X***	Field separator

Host Totals Download Request Message					
Miscellaneous X	Variable Alphanumeric	V		X****	Can contain user defined information.
FS	1 ASCII Char.	F		X****	Field separator
ETX	1 ASCII Char	F	X		End of text Character
LRC	1 Hexadecimal Char	F	X		Longitudinal Redundancy Check. Exclusive OR (XOR) of all characters starting with the first character after the STX, through and including the ETX.

* These fields are optional only as a group. The terminal contains a management function to enable or disable the sending of this group of fields. This group was added in version 2.0, and was made optional in version 2.1 to allow compatibility with older host drivers. If the field group is not enabled on the terminal, these fields will not be sent. If they are not sent, the corresponding fields in the response messages should not be returned.

** This field (Status Monitoring Field) is optional and can be enabled or disabled at the terminal level. If enabled, it is sent on *ALL* messages up to the host. No response is expected to the sending of this information. The first character of the Status Monitoring Field will always be a capital letter (A - Z).

*** This field group (Terminal Totals Fields) is optional and can be enabled or disabled at the terminal level by a management function. If enabled, the Terminal Totals Field is sent with the Host Totals Download Request Message up to the host. The first character, and all characters, of the Terminal Totals Fields will always be numeric (0 – 9).

**** As of version 2.7, multiple Miscellaneous Fields are allowed for. Each field must include a valid FID code and data and be terminated by a field separator. See Valid Misc. FID table.

Host Totals Response Message

Field Name	Length/Type	Fixed/Var.	Reqd	Opt.	Description
STX	1 ASCII Char.	F	X		Start of text character
Information Header	12 ASCII Char.	F		X*	Not used as of this release, must be space filled
FS	1 ASCII Char.	F		X*	Field separator
Terminal ID	15 Alphanumeric	F	X		Terminal ID. Assigned by processor. Left justified, space filled to the right.
FS	1 ASCII Char.	F	X		Field separator
Transaction Code	2 Alphanumeric	F	X		Code indicating type of transaction being done. See Transaction Codes table.
FS	1 ASCII Char.	F	X		Field separator
Business Date	6 Numeric	F	X		Business Date of transactions in MMDDYY format.
FS	1 ASCII Char.	F	X		Field separator
No. of Withdrawals	4 Numeric	F	X		Total number of withdrawals since the last request for totals. Zero or space filled to the left.
No. of Inquiries	4 Numeric	F	X		Total number of inquiries since the last request for totals. Zero or space filled to the left.
No. of Transfers	4 Numeric	F	X		Total number of transfers since the last request for totals. Zero or space filled to the left.
Settlement	8 Numeric	F	X		Total amount of all withdrawals. Zero or space filled to left, right justified. Represents the amount in the smallest possible unit of currency.
FS	1 ASCII Char.	F	X		Field separator
Miscellaneous Field**	Variable alphanumeric	V		X**	Miscellaneous data. Refer to Miscellaneous Field ID codes for possible uses for this field.
FS	1 ASCII Char.	F		X**	Field separator
ETX	1 ASCII Char	F	X		End of text Character
LRC	1 Hexadecimal Char	F	X		Longitudinal Redundancy Check. Exclusive OR (XOR) of all characters starting with the first character after the STX, through and including the ETX.

* These fields are optional only as a group. They should only be included in responses to requests that contain the corresponding optional fields. Refer to the request message table for further information.

** As of version 2.3, only FID 'p' is supported.
 Support for FID '^' was added in version 2.6
 Support for FID 'e' was added in version 2.7   See Valid Misc. FID table.
 Note: 'e' field, if used in this message, contains 12 digit Settlement amount.

Reversal Request Message

Field Name	Length/Type	Fixed/ Var.	Reqd	Opt.	Description
STX	1 ASCII Char.	F	X		Start of text character
Communications Identifier	8 ASCII Char.	F		X*	A text string used to identify the 'owner' of the message to a communications service provider. Default string is "XXXXXX^^". ^ characters are spaces and are required. 'X' characters represent identification string for processor.
Terminal Identifier	2 ASCII Char.	F		X*	Lower case 't' and lower case 'd' or 's', indicating to host the type of terminal
Software Version No.	2 ASCII Char.	F		X*	Two digit Base 36 number representing the version of software installed on the terminal. Starts at '00'
Encryption Mode Flag	1 ASCII Char.	F		X*	0 = Single DES encryption of PIN block. 1 = Reserved. 2 = Triple DES encryption of PIN block.
Information Header	7 ASCII Char.	F		X*	Seven byte field, unused as of this release. Must be space filled.
FS	1 ASCII Char.	F		X*	Field separator
Terminal ID	15 Alphanumeric	F	X		Terminal ID. Assigned by processor. Left justified, space filled to the right.
FS	1 ASCII Char.	F	X		Field separator
Transaction Code	2 Alphanumeric	F	X		"29" for reversal
FS	1 ASCII Char.	F	X		Field separator
Sequence Number	4 Numeric	F	X		Sequence number of the transaction to be reversed.
FS	1 ASCII Char.	F	X		Field separator
Track 2	37 Numeric	V	X		Complete track 2 data, excluding the Start Sentinel, End Sentinel, and LRC
FS	1 ASCII Char.	F	X		Field separator
Amount 1	8 Numeric	F	X		Requested Withdraw amount. Zero filled to the left. Represents the amount in the smallest possible unit of currency.
FS	1 ASCII Char.	F	X		Field separator
Amount 2	8 Numeric	F	X		Surcharge amount as set by terminal. Zero filled to the left. Represents the amount in the smallest possible unit of currency.
FS	1 ASCII Char.	F	X		Field separator
Amount 3	8 Numeric	F	X		Actual Dispensed amount. Zero filled to the left. Represents the amount in the smallest possible unit of currency.
FS	1 ASCII Char.	F	X		Field separator
Status Monitoring Field	XX ASCII Chars.	F	X	X**	Contains status information about terminal. Refer to table for full field format later in this document.
FS	1 ASCII Char.	F		X**	Field separator
Miscellaneous X**	Variable Alphanumeric	V		X***	Miscellaneous data. Refer to Miscellaneous Field ID codes for possible uses for this field.

Reversal Request Message

FS**	1 ASCII Char.	F		X***	Field separator.
ETX	1 ASCII Char	F	X		End of text Character
LRC	1 Hexadecimal Char	F	X		Longitudinal Redundancy Check. Exclusive OR (XOR) of all characters starting with the first character after the STX, through and including the ETX.

* These fields are optional only as a group. The terminal contains a management function to enable or disable the sending of this group of fields. This group was added in version 2.0, and was made optional in version 2.1 to allow compatibility with older host drivers. If the field group is not enabled on the terminal, these fields will not be sent. If they are not sent, the corresponding fields in the response messages should not be returned.

** This field (Status Monitoring Field) is optional and can be enabled or disabled at the terminal level. If enabled, it is sent on *ALL* messages up to the host. No response is expected to the sending of this information. The first character of the Status Monitoring Field will always be a capital letter (A - Z).

*** As of version 2.7, multiple Miscellaneous Fields are allowed for. Each field must include a valid FID code and data and be terminated by a field separator. See Valid Misc. FID table.

Reversal Response Message

Field Name	Length/Type	Fixed / Var.	Reqd	Opt.	Description
STX	1 ASCII Char.	F	X		Start of text character
Information Header	12 ASCII Char.	F		X*	Not used as of this release, must be space filled
FS	1 ASCII Char.	F		X*	Field separator
Terminal ID	15 Alphanumeric	F	X		Copied from request message.
FS	1 ASCII Char.	F	X		Field separator
Transaction Code	2 Alphanumeric	F	X		"29" from request message.
FS	1 ASCII Char.	F	X		Field separator
Sequence Number	4 Numeric	F	X		Copied from request message.
FS	1 ASCII Char.	F	X		Field separator
Response Code	3 Numeric	F	X		Result of request. Approved = 000. 111 = declined.
FS	1 ASCII Char.	F	X		Field separator
Miscellaneous X**	Variable Alphanumeric	V		X**	Miscellaneous data. Refer to Miscellaneous Field ID codes for possible uses for this field.
FS	1 ASCII Char.	F		X**	Field separator, needed only if Miscellaneous field X is present.
ETX	1 ASCII Char	F	X		End of text Character
LRC	1 Hexadecimal Char	F	X		Longitudinal Redundancy Check. Exclusive OR (XOR) of all characters starting with the first character after the STX, through and including the ETX.

* These fields are optional only as a group. They should only be included in responses to requests that contain the corresponding optional fields. Refer to the request message table for father information.

** As of version 2.7, multiple Miscellaneous Fields are allowed for. Each field must include a valid FID code and data and be terminated by a field separator.   See Valid Misc. FID table.

Status Monitoring Field

Sub-Field Name	Length/Type	Description
Program Version Number	10 ASCII Chars.	Program version number in format XX-YYYY.ZZ, where XX indicates product, YYYY indicates processor version, and ZZ indicates revision level. For PC Based products the format is XXMMNNNRRR, where XX = Product Code, MM = Major Version Number, NNN = Minor Version Number, RRR = Revision Version. Refer to table for product identification.
Table Version Number	10 ASCII Chars.	Table version number in format XX-YYYY.ZZ, where XX indicates product, YYYY indicates processor version, and ZZ indicates revision level. For PC Based products the format is XXYYYYZZZZ, where XX = Product Code, YYYY = Screen File ID (alpha-numeric), ZZZZ = Screen File Version. Refer to table for product identification.
Firmware Version Number	10 ASCII Chars.	EPROM version number in format WWXX.YYZAA, where WW is the family product code, XX is the major version number, YY is the minor version number, Z indicates presence of Electronic Journal (security module), and AA is revision of security module firmware For PC Based products the format is WWXX.YYAAA, where WW = Product Code, XX = Main Board Major Version Number, YY = Main Board Minor Version Number, and AAA is revision of security module firmware.
Alarm, Chest door open	1 ASCII Char.	0 – False, 1 – True, <Space> - Not supported, X – Not installed
Alarm, Top door open	1 ASCII Char.	0 – False, 1 – True, <Space> - Not supported, X – Not installed
Alarm, Supervisor active	1 ASCII Char.	0 – False, 1 – True, <Space> - Not supported
Receipt printer, paper status	1 ASCII Char.	0 – OK, 1 – Low, 2 - Out, <Space> - Not supported
Receipt printer, ribbon status	1 ASCII Char.	0 – OK, 1 – Low, 2 - Out, <Space> - Not supported, T – thermal
Journal printer, paper status	1 ASCII Char.	0 – OK, 1 – Low, 2 - Out, <Space> - Not supported, X – Not installed
Journal printer, ribbon status	1 ASCII Char.	0 - OK, 1 – Low, 2 - Out, <Space> - Not supported, T – thermal, X – Not installed
Note status, dispenser	1 ASCII Char.	0 - OK, 1 – Low, 2 - Out, <Space> - Not supported (This is the cumulative summary of all cassettes in the dispenser. Empty individual cassettes are not reflected here).
Receipt printer	1 ASCII Char.	0 - OK, 1 – Needs attention, 2 - Out of service, <Space> - not supported, X - Not installed
Journal Printer	1 ASCII Char.	0 - OK, 1 – Needs attention, 2 - Out of service, <Space> - not supported, X - Not installed
Dispenser	1 ASCII Char.	0 - OK, 1 – Needs attention, 2 - Out of service, <Space> - not supported, X - Not installed
Communications System	1 ASCII Char.	0 - OK, 1 – Needs attention, 2 - Out of service
Card reader	1 ASCII Char.	0 - OK, 1 – Needs attention, 2 - Out of service
Cards retained	3 ASCII Char.	000-999, <Spaces> - Not supported
Electronics system	2 ASCII Chars.	XX represents status of electronics subsystem (Refer to table for listing of codes), <Spaces> - Not supported.
Current Error Code for Terminal	3 ASCII Chars.	XXX represents the value of the error code that existed in the terminal at the time the message was sent. '000' indicates no problems.
Communications failures	3 ASCII Chars.	Number of communications problems experienced since last reset of this value. Comms. Failure would be BUSY, NO CONNECT, etc.
Cassette A Denomination	3 ASCII Chars.	000 - 99K. Values that are all numeric represent actual value of notes. Values suffixed with 'K' indicate thousands. (01K = 1 thousand unit note, 50K = 50

		thousand unit note).
Cassette A notes loaded	4 ASCII Chars.	0000 – 9999. Numbers of notes in the cassette when it was installed. (Note: this values is manually entered).
Cassette A notes dispensed	4 ASCII Chars.	0000 – 9999
Cassette A reject events	3 ASCII Chars.	000 – 999
Cassette B Denomination	3 ASCII Chars.	000 - 99K. Values that are all numeric represent actual value of notes. Values suffixed with 'K' indicate thousands. (01K = 1 thousand unit note, 50K = 50 thousand unit note).
Cassette B notes loaded	4 ASCII Chars.	0000 – 9999. Numbers of notes in the cassette when it was installed. (Note: this values is manually entered).
Cassette B notes dispensed	4 ASCII Chars.	0000 – 9999
Cassette B reject events	3 ASCII Chars.	000 – 999
Cassette C Denomination	3 ASCII Chars.	000 - 99K. Values that are all numeric represent actual value of notes. Values suffixed with 'K' indicate thousands. (01K = 1 thousand unit note, 50K = 50 thousand unit note).
Cassette C notes loaded	4 ASCII Chars.	0000 – 9999. Numbers of notes in the cassette when it was installed. (Note: this values is manually entered).
Cassette C notes dispensed	4 ASCII Chars.	0000 – 9999
Cassette C reject events	3 ASCII Chars.	000 – 999
Cassette D Denomination	3 ASCII Chars.	000 - 99K. Values that are all numeric represent actual value of notes. Values suffixed with 'K' indicate thousands. (01K = 1 thousand unit note, 50K = 50 thousand unit note).
Cassette D notes loaded	4 ASCII Chars.	0000 – 9999. Numbers of notes in the cassette when it was installed. (Note: this values is manually entered).
Cassette D notes dispensed	4 ASCII Chars.	0000 – 9999
Cassette D reject events	3 ASCII Chars.	000 – 999
Total notes purged	3 ASCII Chars.	000 - 999. Total notes exiting the dispenser in response to a purge command. Cassette origin is unknown for these notes.

This field is composed of individual subfields and is sent as a whole group, if enabled. Individual fields cannot be sent separately.

The first character of the Status Monitoring Field will always be a capital letter A(ASCII Char 41h) through Z(ASCII Char 5Ah).

Product Code Table for Program / Table Version Numbers

CODE	DESCRIPTION
C'X'	Model 9500 family of single cassette dispensers. 'X' may be any letter.
D'X'	Model 9515 family of multiple cassette dispensers. 'X' may be any letter.
N'X'	Model 2000 Mako family. 'X' may be any letter.
P'X'	Model 9200 SuperScrip family. 'X' may be any letter.
S'X'	Model 9600 family of single cassette dispensers. 'X' may be any letter.
U'X'	Model 9640 family of single or multiple cassette dispensers. 'X' may be any letter.
T'X'	Model 9615 family of multiple cassette dispensers. 'X' may be any letter.
Z'X'	Model 9700 family of multiple cassette dispensers. 'X' may be any letter.
K'X'	Model 9100 family of single cassette dispensers. 'X' may be any letter.
W'X'	Model 9800 family of single or multiple cassette dispensers. 'X' may be any letter.
X'X'	Model 9600 family of single or multiple cassette dispensers. 'X' may be any letter.
R'X'	PC Based Products family of single or multiple cassette dispensers. 'X' may be any letter.

Product Code Table for EPROM Version Numbers

CODE	DESCRIPTION
C'X'	Model 9500 family of single or multiple cassette dispensers. 'X' may be any letter.
N'X'	Model 2000 Mako and Model 9200 SuperScrip. 'X' may be any letter.
S'X'	Model 9600 family of single or multiple cassette dispensers. 'X' may be any letter.
Z'X'	Model 9700 family of single or multiple cassette dispensers. 'X' may be any letter.
K'X'	Model 9100 family of single cassette dispensers. 'X' may be any letter.
R'X'	PC Based Products family of single or multiple cassette dispensers. 'X' may be any letter.

Transaction Code Table

CODE	DESCRIPTION
01	Change PIN. Must send PIN Change PIN Block (Misc. field) along with this code.
11	Cash Withdrawal from primary checking account
12	Cash Withdrawal from primary savings account
15	Cash Withdrawal from primary credit card account
21	Transfer from primary checking account to savings account
22	Transfer from primary savings account to checking account
25	Transfer from primary credit card account to primary checking account
29	Reverse Previous Withdrawal
31	Primary checking account balance inquiry
32	Primary Savings account balance inquiry
35	Primary Credit card balance inquiry
41	Non-Cash Withdrawal from primary checking account (POS type transaction)
42	Non-Cash Withdrawal from primary savings account (POS type transaction)
43[†]	Quasicash pinless purchase from primary credit account (POS type transaction)
44[†]	Non-Financial prepaid online transaction (POS type transaction)
45	Non-Cash Withdrawal from primary credit card account (POS type transaction)
46†	Send Money from Checking
47†	Send Money from Savings
48†	Check Cashing Withdrawal
49†	Receive Money
50	Get host totals (do not change business day or reset totals)
51	Get host totals (Change business date and reset totals)
52	Recharge existing long distance calling plan.
53	Purchase new long distance calling plan. Use with misc. field 'xr'.
60	Download configuration table
61	Cash Withdrawal from primary checking account using Miscellaneous Field ID 'e' in request message for amount. Amount field 1 is set to spaces.
62	Cash Withdrawal from primary savings account using Miscellaneous Field ID 'e' in request message for amount. Amount field 1 is set to spaces.

	Transaction Code Table
65	Cash Withdrawal from primary credit card account using Miscellaneous Field ID 'e' in request message for amount. Amount field 1 is set to spaces.
71	Transfer from primary checking account to savings account using Miscellaneous Field ID 'e' in request message for amount. Amount field 1 is set to spaces.
72	Transfer from primary savings account to checking account using Miscellaneous Field ID 'e' in request message for amount. Amount field 1 is set to spaces.
75	Transfer from primary credit card account to checking account using Miscellaneous Field ID 'e' in request message for amount. Amount field 1 is set to spaces.
81	Primary checking account balance inquiry using Miscellaneous Field ID 'e' for balance. Amount 1 field in response is set to spaces.
82	Primary savings account balance inquiry using Miscellaneous Field ID 'e' for balance. Amount 1 field in response is set to spaces.
85	Primary credit card balance inquiry using Miscellaneous Field ID 'e' for balance. Amount 1 field in response is set to spaces.
91	Non-Cash Withdrawal from primary checking account (POS type transaction) using Miscellaneous Field ID 'e' in request message for amount. Amount field 1 is set to spaces.
92	Non-Cash Withdrawal from primary savings account (POS type transaction) using Miscellaneous Field ID 'e' in request message for amount. Amount field 1 is set to spaces.
95	Non-Cash Withdrawal from primary credit card account (POS type transaction) using Miscellaneous Field ID in request message 'e' for amount. Amount field 1 is set to spaces.
99[†]	Use Extended Transaction Code String – Miscellaneous FID 'l' (ASCII 6Ch).

†**Preliminary**.

Authorization Codes Table

CODE	DESCRIPTION
000	Transaction approved
001	Expired card
002	Unauthorized usage
003	PIN error
004	Invalid PIN
005	Bank unavailable
006	Card not supported
007	Insufficient funds
008	Ineligible transaction
009	Ineligible account
010	Number of daily withdrawals exceeded
011	Cannot process transaction
012	Amount too large
013	Account closed
014	PIN tries exceeded
015	Database problem
016	Withdrawal limit already reached
017	Invalid amount
018	External decline
019	System error
020	Contact card issuer
021	Routing lookup problem
022	Message edit error
023	Transaction not supported
024	Insufficient funds
025	Western Union sender data error
026	Western Union receiver data error
027	CRC error
028	Pre-pay transaction failed
029	Pre-pay transaction rejected

	Authorization Codes Table	
CODE	**DESCRIPTION**	
030	Invalid mobile phone number	
031	Pre-pay account limit reached	
032	Pre-pay system unavailable	
033	Response would exceed message size limit	
034	Necessary information missing to process transaction	
035	Second Invalid PIN (second "invalid PIN" try in a row and one try is left before deactivation)	
111	Reversal Declined	
222	PIN Change Declined	

Miscellaneous Field ID Descriptions

Field ID Code	DESCRIPTION
'!' (exclamation point)	Surcharge amount to be displayed to customer during Surcharge Notification screen. 8 numeric ASCII characters, right justified and zero filled to the left. Represents the amount in the smallest possible unit of currency. Amount cannot be above "00032767"
'/' (solidus)	MAC enable or disable field. 1 ASCII Character. An ASCII '0' disables MAC (disabled by default) and an ASCII '1' enables MAC. The MAC disable field '/0' is not allowed in Configuration Download Response Messages.
'^' (caret)	MAC (Message Authentication Code) Result. 9 ASCII characters calculated with the MAC key by encrypting the message starting from the STX and ending with the ETX, the LRC is ignored. The MAC is separated into two equal halves by an ASCII space. MAC result example: 'A562 34CD'. NOTE: Sending a MAC with 9 ASCII spaces will cause the terminal to fail the current message and perform a Configuration Table Download on the next call.
'b'	Supplemental balance field, 8 numeric ASCII characters long zero filled to left. Eleven space characters are used to pad the field to 20 positions. Example: [b00123456_ _ _ _ _ _ _ _ _ _ _] where '00123456' is 123456 units of available balance. Represents the amount in the smallest possible unit of currency.
'c'	Day close time is the time of day specified in hours and minutes when the scheduled day close will occur. The format is HHMM. The valid range is 0000(midnight) to 2359.
'd'	Message Download is used to download the programmable messages to the terminal. The first character after the FID is a character that defines which type of message is to be downloaded. The four message types currently supported are **s**tore, **m**arketing, **w**elcome and **e**xit. The first letter of each message type is used to identify it after the FID. The second character after the FID is the number of lines contained in the message. The text format is any ASCII character of 20 hex or greater. A maximum of 163 characters, including FID, message identifier, and line count, is allowed for the store and marketing messages. A maximum of 93 characters, including FID, message identifier, and line count, is allowed for welcome and exit messages. The following table lists the message types with associated REQUIRED line lengths.

Message Type	Message Identifier	Max. no. of Lines	Required number of characters per line
Store	s	4	40
Marketing	m	4	40
Welcome	w	3	30
Exit	e	3	30

Field ID Code	DESCRIPTION
'e'	Extended length amount field. When present in a Transaction Request Message, this field OVERRIDES the amount field 1 in the response message. Amount 1 will be space filled to indicate this. It can be used for balance inquiries. The format consists of the FID code 'e', followed by 12 ASCII digits, zero filled to the left. Example: [e000123456789] where '000123456789' represents 123,456,789 units of currency. (NOTE: the units always represent the smallest possible representation of the currency involved. For United States, this would be the number of pennies). When present in a Host Totals Response Message, this field represents the 12 digit Settlement Amount.
'&'	28 Digit Account Number (i.e. Checking, Savings, etc.) Left justified, padded with spaces.
'#'	12 Digit (alphanumeric) Sequence Number.
'@'	PIN Change PIN Block. 16 alphanumeric. ANSI standard encrypted PIN block. (See Appendix A)
'g'	Track 3 information, excluding the Start Sentinel, End Sentinel, and LRC. If this field is used, and if track 3 data is not present or is unreadable, this field will contain just the FID code 'g'.
'h'	Heartbeat interval (minutes) is the length of time the terminal will sit idle (no transactions initiated) before it sends a Configuration Download Request. The format is 3 ASCII numeric characters, right justified and zero filled to the left. The valid range is 1 to 999.

Miscellaneous Field ID Descriptions

'i' ASCII Char – 69h.	Primary Account Number from track 3 on the magnetic stripe. If this field is used, and if track 3 data is not present or is unreadable, this field will contain just the FID code 'i'.
'k'	Issuer Fee/Credit to be displayed to customer during Surcharge Notification screen. Nine numeric ASCII characters, right justified and zero filled to the left. Represents the amount in the smallest possible unit of currency. An ASCII minus sign (e.g. "-00000100") in the first position represents a credit. The absence of this field implies an unknown Issuer Fee/Credit.
'l' † ASCII Char – 6Ch.	Extended Transaction Code String. – Six ASCII numbers. – $T_1 T_2 T_3 T_4 T_5 T_6$ 2 Numeric ($T_1 T_2$) - Transaction Type Code 2 Numeric ($T_3 T_4$) - "From" Account Type Code (Code '00' not allowed) 2 Numeric ($T_5 T_6$) - "To" Account Type Code See Appendix C – Extended Transaction Code Table for a list of Transaction and Account Type Codes.
'm'	MAC (Message Authentication Code) key. 16 ASCII characters encrypted under Master key. Will be used starting with the *next* transaction.
	MAC (Message Authentication Code) Working Key Left Block for Triple-DES capable terminals. 16 ASCII characters encrypted under MAC Master key. Each character represents a 4-bit hexadecimal numeral (0-9, A-F). See APPENDIX E for the complete description of Encryption key sets. Will be used starting with the *next* transaction. 　　　The presence of only this FID in a Response Message (Transaction or Configuration Table Download) will enable Single-DES MAC Encryption.
'n'	Reason for reversal. Two ASCII numbers representing the following reasons for a reversal: '01' - Incorrect Dispense: The amount dispensed does not match amount requested. This may be due to either a mechanical failure or the lack of available bill(s) to make the requested amount. '02' – Protocol Error: A request message was sent from the terminal for which no valid response message was received from the host. '03' – Lost EOT: A valid response message was received by the terminal, but the EOT was not received. This assumes the terminal was configured to expect the EOT. If the terminal is configured to ignore EOT, there will be no reversal generated. '04' – Mac Error: The calculated MAC result does not match the MAC result returned in the response message. '05' - Customer Cancellation: Customer decided not to continue after reviewing the transaction fee. '06' – VAS Challenge/Response Error. An incorrect response was received in the 'vd' FID. '07' – ICC declined transaction.

Miscellaneous Field ID Descriptions

'o' † ASCII Char – 6Fh.	Total number of CREDIT ADVANCE transactions and the total amount of all CREDIT ADVANCE transactions. (12 Numeric total) 4 Numeric – Total number of CREDIT ADVANCE transactions since the last request for totals. Zero filled to the left. 8 Numeric – Total amount of all CREDIT ADVANCE transactions. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.
'p'	ASCII formatted printing text field. This field, if present, will be printed at the end of a successful transaction receipt, error receipt or host totals receipt. It must include as the second character (after the 'p') the number of lines to be printed (from '1' to '4'). Preformatted text follows this line count. All ASCII characters above 20 HEX (the space character) are allowed. The only control character allowed is the carriage return, 0d HEX. The printer is capable of printing up to forty characters per line. Each separate line of text must be terminated by a carriage return. No centering is done by the terminal; all text is printed as sent. Maximum length of this field is 166 characters, including the 'p'. Can also appear in host totals response message
't'	Current network time sent from the host processor to update the terminal's time. The format is 6 numeric ASCII characters in the form HHMMSS. The time will be in 24 hour military format. May be used with the 'ua' FID to update both the time and date of the terminal. If the terminal software does not support the 'ua' FID, send the 't' FID alone to update only the terminal's time. Both the time and date must reflect the local time zone of the terminal.

'u' ASCII Char – 75h.		Two character FIDs. The first character after the FID 'u' is another character that defines which data element is to be transmitted. The table below describes each data element. A Field Separator must follow each field.
	'a'	Current network date sent from the host processor to update the terminal's date. The format is 6 numeric ASCII characters in the form MMDDYY. The date format is month, day, year. Must be used with the 't' FID to update both the time and date of the terminal. Both the time and date must reflect the local time zone of the terminal.
	'b'	16-bit CRC. 4 ASCII characters that represent the CRC-16 two byte checksum. Each character represents a 4-bit hexadecimal numeral (0-9, A-F). Uses the ANSI CRC-16 error checking protocol standard. For a request message the 16-bit CRC calculation starts with the first character after the STX, and ends with the last character before the ETX, includes four ASCII zeros for the 'ub' field, and excludes the LRC. The result is the four ASCII characters that is placed in the 'ub' field in msb to lsb order. The host must also calculate the CRC by substituting the four ASCII character CRC result in the 'ub' field with four ASCII zeros, then compare the results. The converse should be performed for the response message. The Triton TCP/IP protocol does not contain an STX, ETX, nor LRC, and excludes the optional two-byte TCP/IP message length. See APPENDIX F for the complete ANSI 16-bit CRC description.
	'd'	Encoded EMV data block ASCII characters. Variable length. See appendix G for description of the formatting of this data field

Miscellaneous Field ID Descriptions

	'e'	DATA Working Key Left Block.
		16 ASCII characters. Each character represents a 4-bit hexadecimal numeral (0-9, A-F).
		See APPENDIX E for the complete description of Encryption key sets.
		Will be used starting with the *next* transaction.
	'f'	DATA Working Key Right Block.
		16 ASCII characters. Each character represents a 4-bit hexadecimal numeral (0-9, A-F).
		See APPENDIX E for the complete description of Encryption key sets.
		Will be used starting with the *next* transaction.
	'g'	Host Transaction Trace Number
		12 ASCII characters. Fixed length. Right justified, space filled to the left if less than 12 characters.
	'h'	Encoded EMV untagged-data block
		ASCII characters. Variable length.
		See appendix G for description of the formatting of this data field.
	'i'	Motorized card reader commands
		2 Numeric characters. Fixed length.
		This field is indented for use only on ATM's that have a motorized card reader.
		01 – Capture card. This command holds the customer's card inside a motorized card reader.
'v' ASCII Char – 76h.		Generic Value Added Service(VAS) fields.
		The first character after the FID 'v' is another character that defines which data element is to be transmitted. The table below describes each data element. A Field Separator must follow each field.
	'a'	Value Added Service Terminal ID.
		15 ASCII characters. Space filled to the right.
	'b'	Postal code of Terminal for Value Added Service.
		12 ASCII characters. Space filled to the right.
	'c'	Loyalty card information for Value Added Service.
		80 ASCII characters maximum. Variable length.
	'd'	VAS Challenge/Response used in transaction request/response messages.
		20 ASCII characters. Each character represents a 4-bit hexadecimal numeral (0-9, A-F).
		You must obtain a four-digit Triton-waves identification number and a Triton-waves encryption key from Triton Systems. The ATM sends a twenty-digit hexadecimal string to the Triton-waves host processor in a transaction request. The first four digits should be ignored. The processor should DES encrypt the last sixteen digits with the Triton-waves encryption key. Then, the processor should place its four-digit Triton-waves identification number in the first four positions of the response string and the sixteen-digit encryption result in the last sixteen positions, and send the entire twenty-digit string to the ATM in a transaction response. Transactions that have an incorrect response will be reversed. The Triton-waves encryption key will be changed on a yearly basis.
'w'		Maximum withdrawal amount is the largest dollar amount allowed for a withdrawal transaction. The format is 3 ASCII numeric characters right justified and zero filled to the left. The valid range is $1 to $999. This does not override any maximum set by the network.
'x' [†] ASCII Char – 78h.		Prepaid online and/or prepaid offline fields.
		The first character after the FID 'x' is another character that defines which data element is to be transmitted. The table below describes each data element. A Field Separator must follow each field.
	'a'	Telco-product Serial Number for prepaid offline transactions.
		16 ASCII characters maximum

		Miscellaneous Field ID Descriptions
	'b'	User's mobile phone number for prepaid offline or online transactions when used in a transaction request. Activation phone number for prepaid offline or online transactions when used in a transaction response. 20 ASCII characters maximum
	'c'	Taxes 1 – (GST/HST/PST – General Sales Tax / Harmonized Sales Tax / Provencial Sales Tax for offline transactions) or general taxes for offline transactions. 8 numeric Zero filled to the left. Represents the amount in the smallest possible unit of currency.
	'd'	Taxes 2 – General taxes for online transactions. 8 numeric Zero filled to the left. Represents the amount in the smallest possible unit of currency. The value sent in a transaction request is the total tax as calculated by the ATM, and the value received in the transaction response will be printed to the customers receipt. Amount cannot be above "00032767".
	'e'	Total number of prepaid online transactions and the total amount of all prepaid online transactions. (12 Numeric total) 4 Numeric – Total number of Wireless Phone Refill transactions since the last request for totals. Zero filled to the left. 8 Numeric – Total amount of all Wireless Phone Refill transactions. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.
	'f'	Contact phone number for prepaid online transactions. 20 ASCII characters maximum
	'g'	Service provider Name for prepaid online transactions. 20 ASCII characters maximum
	'h'	6 Digit (numeric) Expiration date (MMDDYY) for online transactions.
	'i'	Secret Number for prepaid offline transactions 20 ASCII characters maximum
	'n'	Actual amount debited from the customer's account for online transactions. 8 Digit (numeric) Zero filled to the left. Represents the amount in the smallest possible unit of currency.
	'p'	Voucher PIN number for online transactions. 25 ASCII characters maximum
	'q'	Service provider name and fast cash amounts for wireless transactions. - 82 bytes maximum 24 Alphanumeric max – (required) Service provider name – (variable length). 1 RS character – (required) 0x1E 1 Numeric – (required) 1=enable provider name, 0=disable provider name. 1 RS character – (optional if disabling provider name) 0x1E 48 Numeric – (optional if disabling provider name) Six fast cash amounts, each amount is 8 Numeric characters. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency. 1 RS character – (optional - based on implementation) 0x1E 6 Numeric – (optional - based on implementation) Service provider ID An ASCII zero alone in the service provider name will disable all previous programmed service provider names and fast cash amounts. Example: xq0 Rs 0

Miscellaneous Field ID Descriptions

	'r'		Purchase new long distance calling plan. Used when the transaction code is "53". 01 – US calling – penny plan. 02 – US calling – long talk plan. 03 – US calling – short talk plan. 04 – US calling – best value plan. 05 – Mexico calling – long talk plan. 06 – Mexico calling – short talk plan. 07 – Mexico calling – best value plan. 08 – International calling – long talk plan. 09 – International calling – short talk plan. 10 – International calling – best value plan.
	's'		Total number of long distance transactions and the total amount of all long distance transactions. (12 Numeric total) 4 Numeric – Total number of long distance transactions since the last request for totals. Zero filled to the left. 8 Numeric – Total amount of all long distance transactions. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.
	't'		Tax rate – General tax rate for wireless or long distance transactions. 4 numeric. Zero filled to the left. Represents a percentage from 00.00% to 99.99%. The decimal should not be included in the field. Amount cannot be above "9999". Will be used starting with the *next* transaction.
	'u'		Service provider ID. 6 numeric. fixed length.
	'v'		Service provider transaction totals and amounts. (18 Numeric total) 6 Numeric – Service Provider ID. 4 Numeric – Total number of service provider transactions since the last request for totals. Zero filled to the left. 8 Numeric – Total amount of all service provider transactions. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.
'y' [†] ASCII Char – 79h.			Bill Payment, Electricity Prepaid, and Check Cashing fields.
			The first character after the FID 'y' is another character that defines which data element is to be transmitted. The table below describes each data element. A Field Separator must follow each field.
	'a'		Bill Payment account or electricity meter number. 39 ASCII characters maximum
	'b'		Receiver name. 35 ASCII characters maximum
	'c'		Check cashing Authorization code. 9 numeric. fixed length
	'd'		Check cashing PIN. 3 to 6 numeric.

		Miscellaneous Field ID Descriptions	
	'e'	Total number of check cashing transactions and the total amount of all check cashing transactions. (12 Numeric total) 4 Numeric – Total number of check cashing transactions since the last request for totals. Zero filled to the left. 8 Numeric – Total amount of all check cashing transactions. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.	
	'f'	Total number of Bill Payment transactions and the total amount of all Bill Payment transactions. (12 Numeric total) 4 Numeric – Total number of Bill Payment transactions since the last request for totals. Zero filled to the left. 8 Numeric – Total amount of all Bill Payment transactions. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.	
'z' [†] ASCII Char – 7Ah.		Funds fields.	
		The first character after the FID 'z' is another character that defines which data element is to be transmitted. The table below describes each data element. A Field Separator must follow each field.	
	'a'	16 Digit (alphanumeric) Encrypted Sender ID for Funds transactions.	
		Sender ID is encrypted as an ANSI standard PIN Block. For receive transactions, code "49", the PIN Block calculation uses a Primary Account Number that has been sent in the 'zn' field. The default value of the receive PAN is sixteen ASCII zeros. For send transactions the card PAN is used for the PIN Block calculation.	
	'b'	9 Digit (numeric) Preferred Customer ID for Funds transactions.	
	'c'	6 Digit (numeric) Confirmation ID for Funds transactions.	
	'd'	8 Numeric – State tax value for Funds transactions. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.	
	'e'	16 ASCII characters. Money Transfer Control Number (MTCN) for Funds transactions.	
	'f'	1 ASCII character. Enable or disable funds field. For Configuration Download Response transaction message: ASCII '0' – Disable funds transactions (disabled by default) ASCII '1' – Enabled funds transactions.	
	'g'	20 ASCII characters maximum. Assistance phone number for Funds transactions.	
	'h'	8 Numeric – Maximum request amount for a Funds Transaction. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.	
	'i'	8 Numeric – Smallest denomination multiple for a Funds Transaction. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.	
	'j'	8 Numeric – Funds convenience fee. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.	
	'k'	Total number of funds-send transactions and the total amount of all funds-send transactions. (12 Numeric total) 4 Numeric – Total number of funds-send transactions since the last request for totals. Zero filled to the left. 8 Numeric – Total amount of all funds-send transactions. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.	

Miscellaneous Field ID Descriptions

	'm'	Total number of funds-receive transactions and the total amount of all funds- receive transactions. (12 Numeric total) 4 Numeric – Total number of funds- receive transactions since the last request for totals. Zero filled to the left. 8 Numeric – Total amount of all funds- receive transactions. Zero filled to left, right justified. Represents the amount in the smallest possible unit of currency.
	'n'	PAN used for Western Union Receive transaction request. 16 Numeric characters.
'~' (tilde) ASCII Char 7Eh	DES Communications key (PIN Working Key). 16 ASCII characters long, encrypted under Master key. Will be used starting with the *next* transaction. Same format as this field in configuration table download. —— Triple-DES Encrypted PIN Key 1 (*K1)* if the terminal is Triple-DES capable (See APPENDIX D). Each character represents a 4-bit hexadecimal numeral (0-9, A-F).	
'{' [†] (left brace) ASCII Char 7Bh	Triple-DES Encrypted PIN Key 2 (*K2)* (See APPENDIX D) when used in a Response Message. 16 ASCII characters. Each character represents a 4-bit hexadecimal numeral (0-9, A-F). The absence of this FID in a Response Message(Transaction or Configuration Table Download) will set K2 equal to K1 (*K2=K1)* and the '[' FID equal to zero(0) for all request messages if the terminal is Triple-DES capable, which is identical to Single-DES encryption of the PIN block. The presence of this FID in a Response Message(Transaction or Configuration Table Download) will set the '[' FID equal to two (2) for all request messages if the terminal is Triple-DES capable. Will be used starting with the *next* transaction.	
'}' [†] (right brace) ASCII Char 7Dh	MAC (Message Authentication Code) Working Key Right Block for Triple-DES capable terminals. 16 ASCII characters encrypted under MAC Master key. Each character represents a 4-bit hexadecimal numeral (0-9, A-F). Will be used starting with the *next* transaction. See APPENDIX E for the complete description of Encryption key sets. The presence of both the 'm' FID and this FID in a Response Message (Transaction or Configuration Table Download) will enable Triple-DES MAC Encryption if the terminal is Triple-DES capable.	
'[' [†] (left bracket) ASCII Char 5Bh	Terminal is Triple-DES capable / Encryption Mode Flag (EMF) (See APPENDIX D) 1 ASCII character. 0(default) = Terminal is Triple-DES capable (reset to zero (0) by absence of the '{' FID in a Transaction or Configuration Table Download message from the host) 2 = Terminal is Triple-DES capable (set to two (2) by the presence of the '{' FID in a Transaction or Configuration Table Download message from the host) Terminals that are not Triple-DES capable will not send this FID, therefore its absence indicates the terminal is Single-DES only. The value of this FID (0 or 2) is also the value of the Encryption Mode Flag in the communication header of request messages.	

This table describes the Field ID codes that can appear in the miscellaneous fields in the response message. In all cases, the Field ID (FID) Code character *must* be the first character in the field, with the appropriate data following directly after the FID. Any field described here may be placed in either field Miscellaneous 1, Miscellaneous 2, or Miscellaneous X, where appropriate.

[†]**Preliminary**.

Valid Miscellaneous Field ID Table

FID 1st char	FID 2nd char	Transaction Message		Config. Message		Host Totals Message		Reversal Message	
		Request	Response	Request	Response	Request	Response	Request	Response
! – 21h		X	X		X				
# - 23h		X	X					X	X
& - 26h		X	X						
/ - 2Fh			X		X				
@ - 40h		X							
[- 5Bh				X		X		X	
^ - 5Eh		X	X			X	X	X	X
{ - 7Bh			X		X				
~ - 7Eh			X		X				
} – 7Dh			X		X				
a									
b			X						
c			X						
d			X						
e		X	X						
f									
g		X						X	
h									
i		X						X	
j									
k			X					X	
l		X	X						
m			X						
n								X	
o						X	X		
p			X				X		
q									
r									
s									
t			X						
	a		X						
	b	X	X	X	X	X	X	X	X
	c								
	d	X	X					X	
u	e		X		X				
	f		X		X				
	g		X				X		X
	h	X	X					X	
	i		X						
v	a	X				X		X	
	b	X						X	

FID 1st char	FID 2nd char	Transaction Message		Config. Message		Host Totals Message		Reversal Message	
		Request	Response	Request	Response	Request	Response	Request	Response
	c	X							
	d	X	X						
w			X						
x	a		X						
	b	X	X						
	c		X						
	d	X	X						
	e					X	X		
	f		X						
	g	X	X						
	h		X						
	i		X						
	n		X						
	p		X						
	q		X		X				
	r	X							
	s					X	X		
	t		X		X				
	u	X						X	
	v					X	X		
y	a	X							
	b	X							
	c	X							
	d	X							
	e					X	X		
	f					X	X		
z	a	X							
	b	X							
	c	X	X						
	d		X						
	e		X						
	f				X				
	g				X				
	h				X				
	i				X				
	j		X						
	k					X	X		
	m					X	X		
	n		X		X				

X = FID Allowed for message type.
See "Miscellaneous Field ID Descriptions" for data format and construction. The highlighted Field IDs are undefined.

PRELIMINARY

PROTOCOL SPECIFICATION

The Triton terminal communications protocol closely follows the VISA II POS Authorization protocol. The following diagrams illustrate the protocol level for messages sent between the terminal and the processor.

Diagrams are provided for the two modes of normal operation (terminal expects EOT, and terminal does not require EOT), as well as conditions that result in cancelled transactions.

PRELIMINARY

Normal Message w/EOT

This diagram illustrates the line protocol for a normal dispense cycle. Dispense occurs after Host EOT is received (default).

Terminal		Host Processor

```
Terminal ─────────────────────────────── Host Processor

┌─────────────────────┐
│  Terminal calls Host │──────────────────────┐
└─────────────────────┘                       │
                                              ▼
                ┌──────────────────┌─────────────────────┐
                │                  │        ENQ          │
                │                  └─────────────────────┘
                ▼
┌─────────────────────────┐
│ STX <REQUEST> ETX LRC   │────────────────┐
└─────────────────────────┘                │
                                           ▼
                        ┌─────────────────────────────┐
                        │  STX <RESPONSE> ETX LRC     │
                        └─────────────────────────────┘
                ▼
┌─────────────────────┐
│        ACK          │──────────────────────┐
└─────────────────────┘                      │
                                             ▼
                        ┌─────────────────────────┐
                        │          EOT            │
                        └─────────────────────────┘
        ▼
┌─────────────────────┐
│        EOT          │──────────────────────┐
│  Modem Disconnect   │                      │
└─────────────────────┘                      ▼
                        ┌─────────────────────────┐
                        │      Disconnect         │
                        └─────────────────────────┘
```
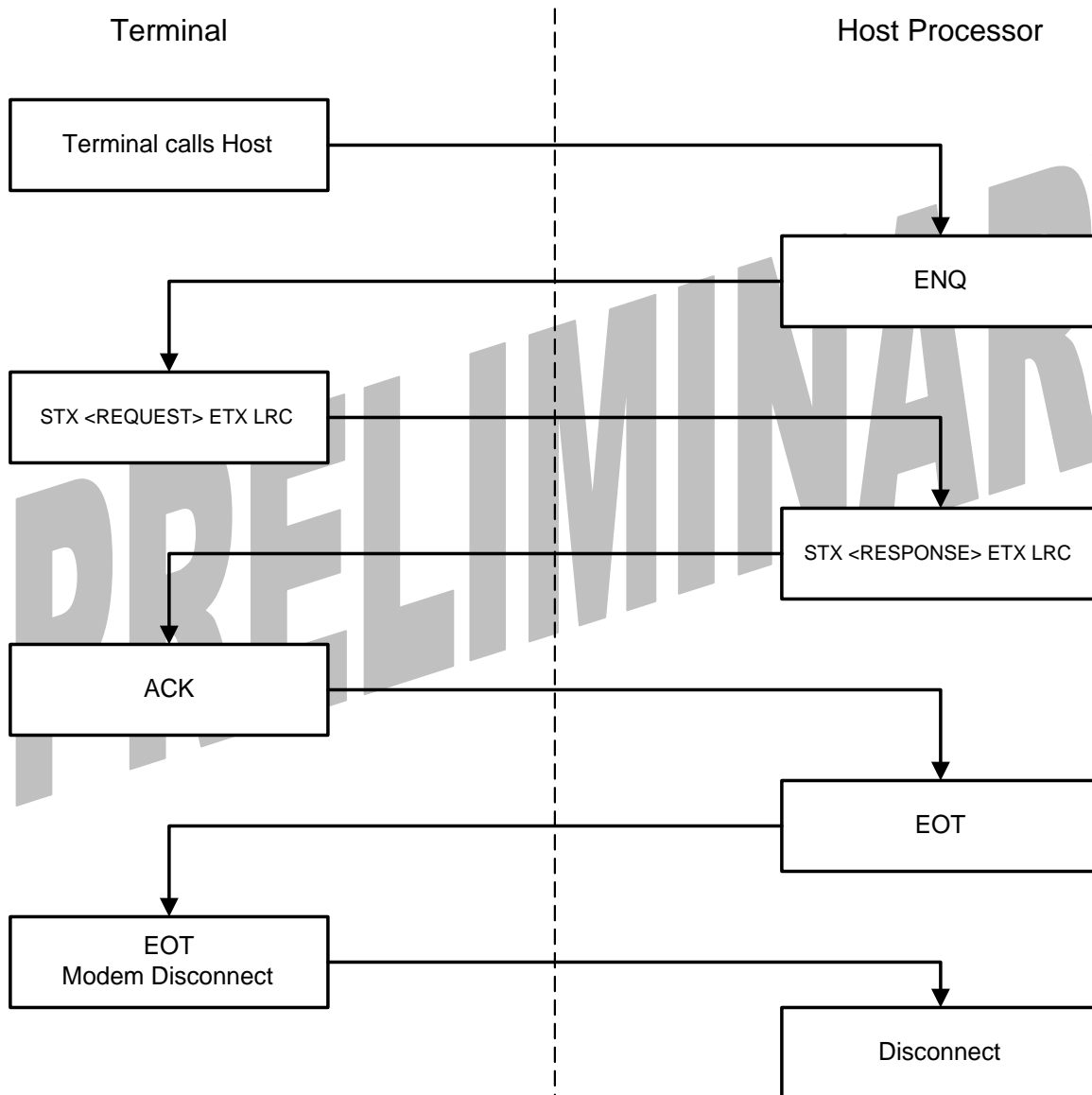
In this mode, the terminal will not dispense unless it receives the EOT from the host.

Normal Message w/o EOT

This diagram illustrates the line protocol for a normal dispense cycle when the terminal is not expecting an EOT. Dispense occurs after the terminal sends the ACK to the HOST. If the host sends an EOT it will be ignored.

Terminal	Host Processor
Terminal calls Host	
	ENQ
STX <REQUEST> ETX LRC	
	STX <RESPONSE> ETX LRC
ACK Modem Disconnect Dispense occurs	
	Disconnect
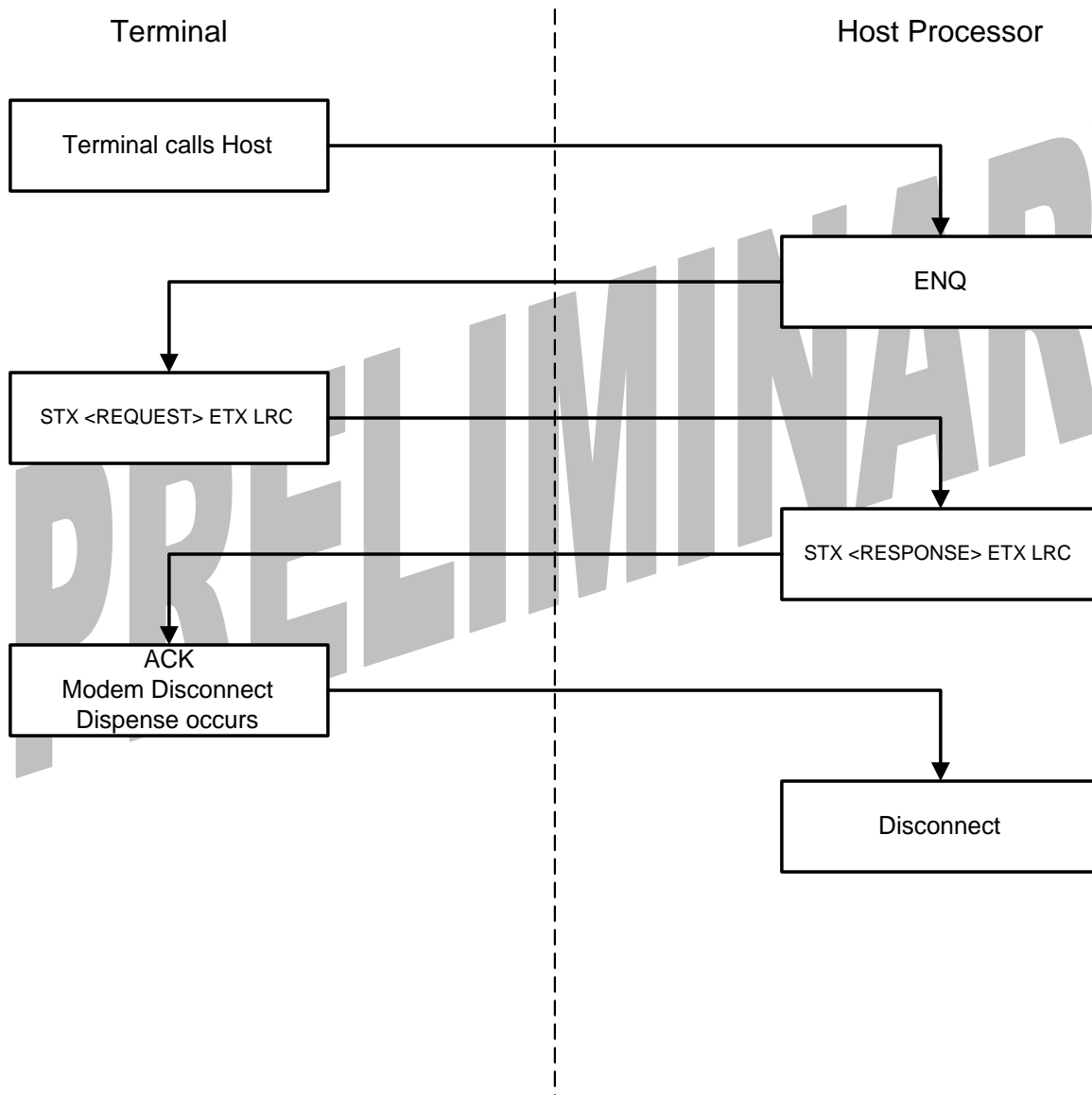
Correctable Request and Response Transmit Error

This diagram illustrates the line protocol for a correctable transmit error in the request and response messages. The NAK character is sent to indicate an error in the LRC.

Terminal   Host Processor

| Terminal calls Host |

| ENQ |

| STX <REQUEST> ETX LRC |

| NAK |

| STX <REQUEST> ETX LRC |

| STX <RESPONSE> ETX LRC |

| NAK |

| STX <RESPONSE> ETX LRC |

| ACK |

| EOT
Disconnect |

| EOT
Modem Disconnect |
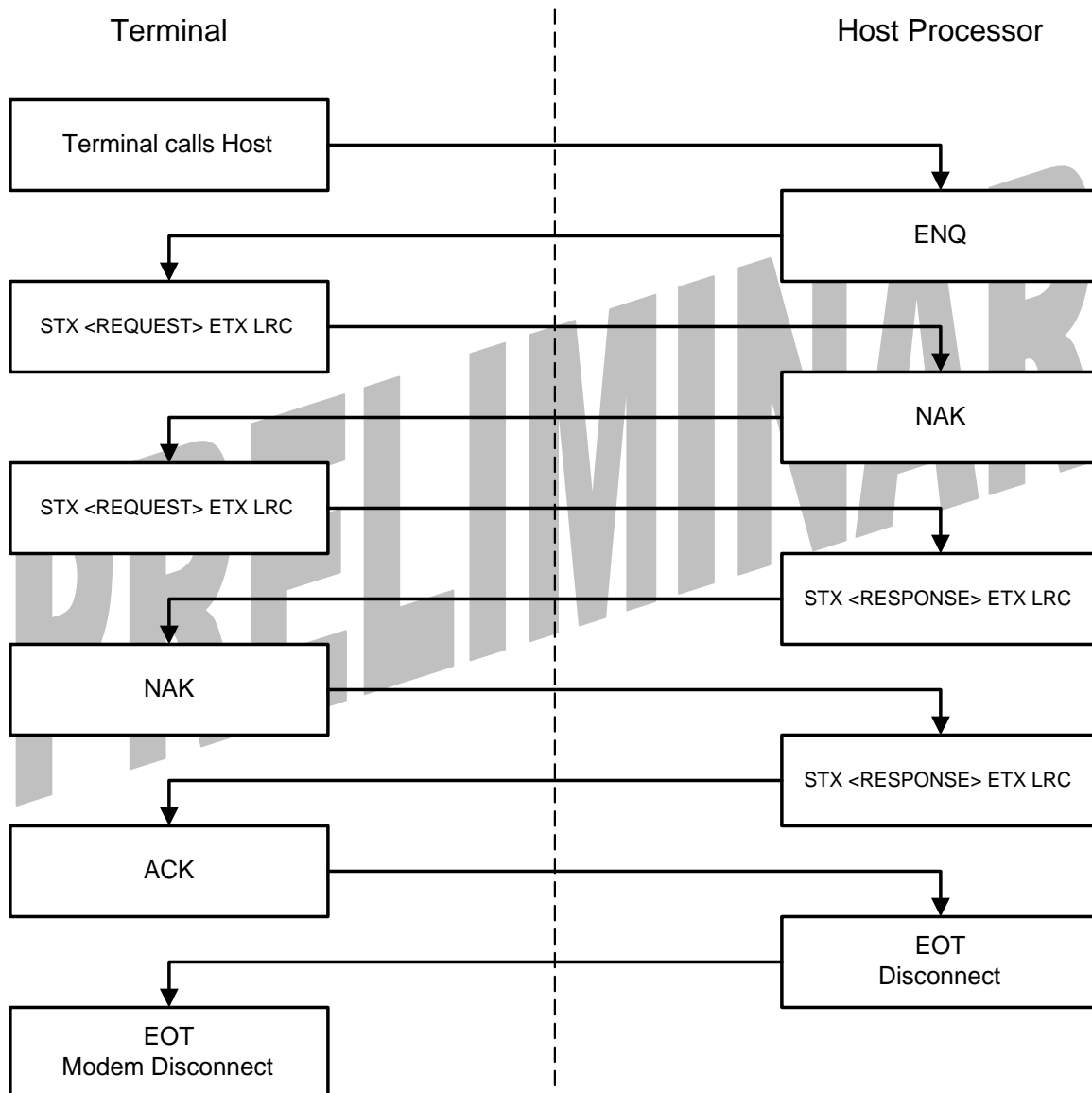
Uncorrectable Request Transmit Error

This diagram illustrates the line protocol for an uncorrectable transmit error in the request message. The NAK character is sent from the host to indicate an error in the LRC. The terminal will not dispense if this happens.

Terminal	Host Processor
Terminal calls Host	
	ENQ
STX <REQUEST> ETX LRC	
	NAK
STX <REQUEST> ETX LRC	
	NAK
STX <REQUEST> ETX LRC	
	NAK
STX <REQUEST> ETX LRC	
	EOT Disconnect
EOT Modem Disconnect Transaction cancelled	
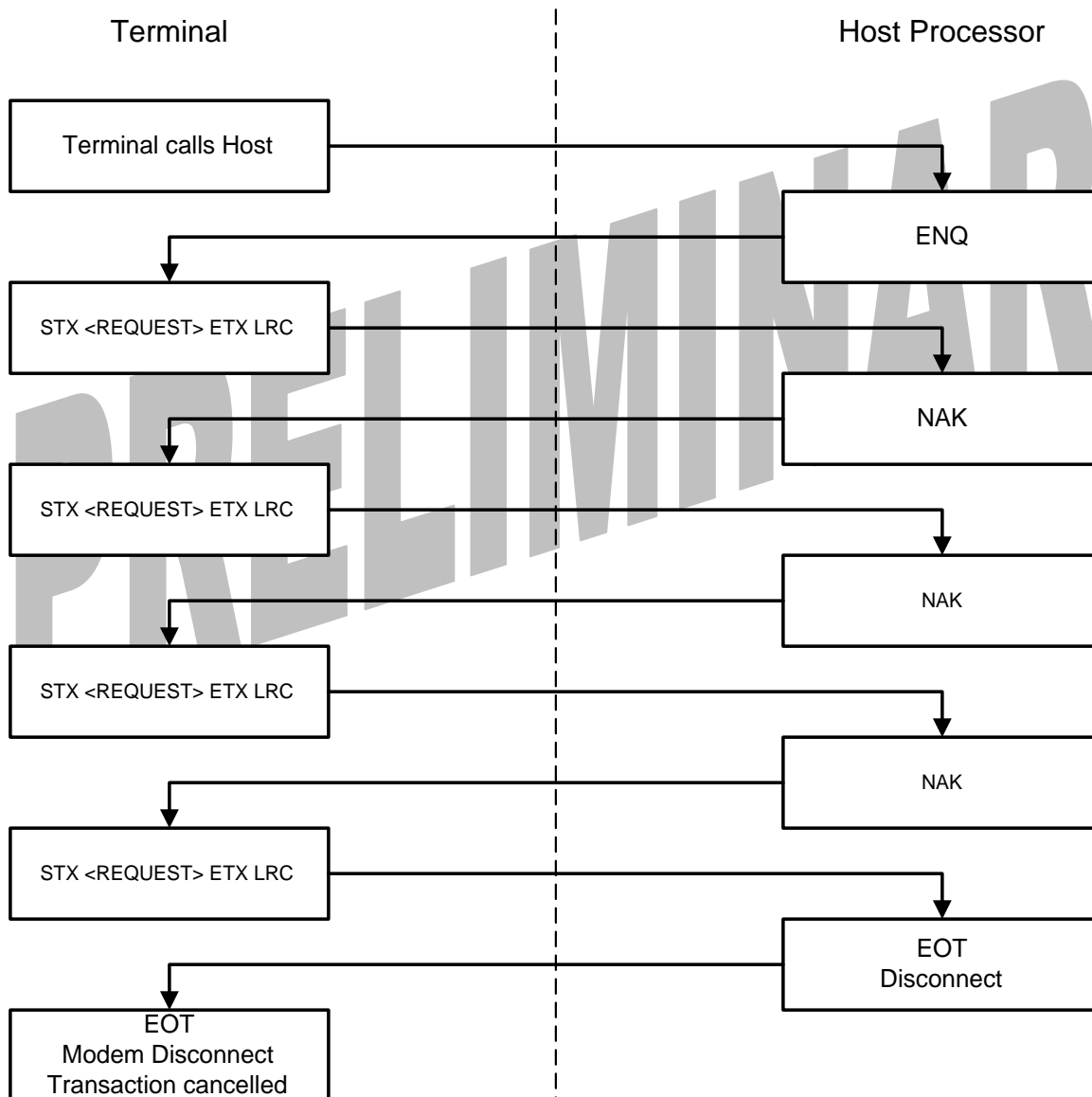
Uncorrectable Response Transmit Error

This diagram illustrates the line protocol for an uncorrectable transmit error in the response message. The NAK character is sent from the terminal to indicate an error in the LRC. The terminal will not dispense if this happens.

Terminal		Host Processor
Terminal calls Host		
		ENQ
STX <REQUEST> ETX LRC		
		STX <RESPONSE> ETX LRC
NAK		
		STX <RESPONSE> ETX LRC
NAK		
		STX <RESPONSE> ETX LRC
NAK		
		EOT Disconnect
EOT Modem Disconnect Transaction cancelled		
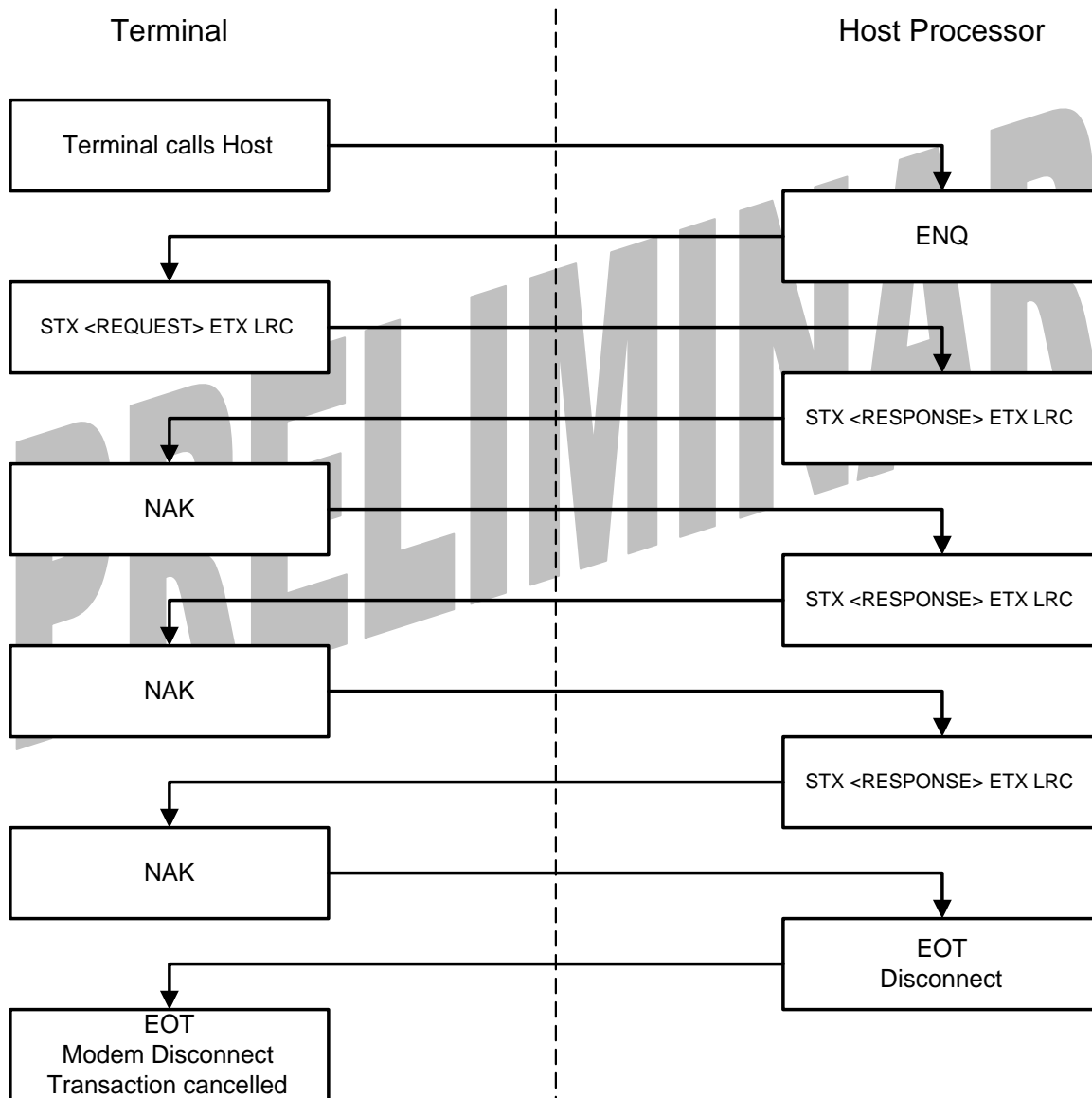
Terminal ACK Not Received By Host

This diagram illustrates the line protocol when the host does not receive the ACK properly. In this scenario, the terminal will not dispense because no EOT was received (assuming the terminal is configured to expect EOT). The host should reverse the transaction.

Terminal	Host Processor

```
┌─────────────────────┐
│ Terminal calls Host  │──────────────────────────────┐
└─────────────────────┘                               ▼
     ┌───────────────────────────────────┐  ┌──────────────────────┐
     ▼                                    │  │        ENQ           │
┌─────────────────────┐                   │  └──────────────────────┘
│ STX <REQUEST> ETX LRC │──────────────────┼────────────┐
└─────────────────────┘                   │            ▼
         ┌─────────────────────────────────┤  ┌──────────────────────┐
         ▼                                 │  │ STX <RESPONSE> ETX LRC │
┌─────────────────────┐   ACK garbled      │  └──────────────────────┘
│        ACK          │────────────────────┘            │ 3 sec.
└─────────────────────┘                                 │ timeout
         ┌──────────────────────────────────┐  ┌──────────────────────┐
         ▼                                  │  │ STX <RESPONSE> ETX LRC │
┌─────────────────────┐   ACK garbled       │  └──────────────────────┘
│        ACK          │─────────────────────┘            │ 3 sec.
└─────────────────────┘                                  │ timeout
         ┌──────────────────────────────────┐  ┌──────────────────────┐
         ▼                                  │  │ STX <RESPONSE> ETX LRC │
┌─────────────────────┐   ACK garbled       │  └──────────────────────┘
│        ACK          │─────────────────────┘            │ 3 sec.
└─────────────────────┘                                  │ timeout
         ┌──────────────────────────────────┐  ┌──────────────────────┐
         ▼                                  │  │     Disconnect       │
┌─────────────────────┐                     └──│     (NO EOT)         │
│        EOT          │                        └──────────────────────┘
│  Modem Disconnect   │
│ Transaction cancelled │
└─────────────────────┘
```
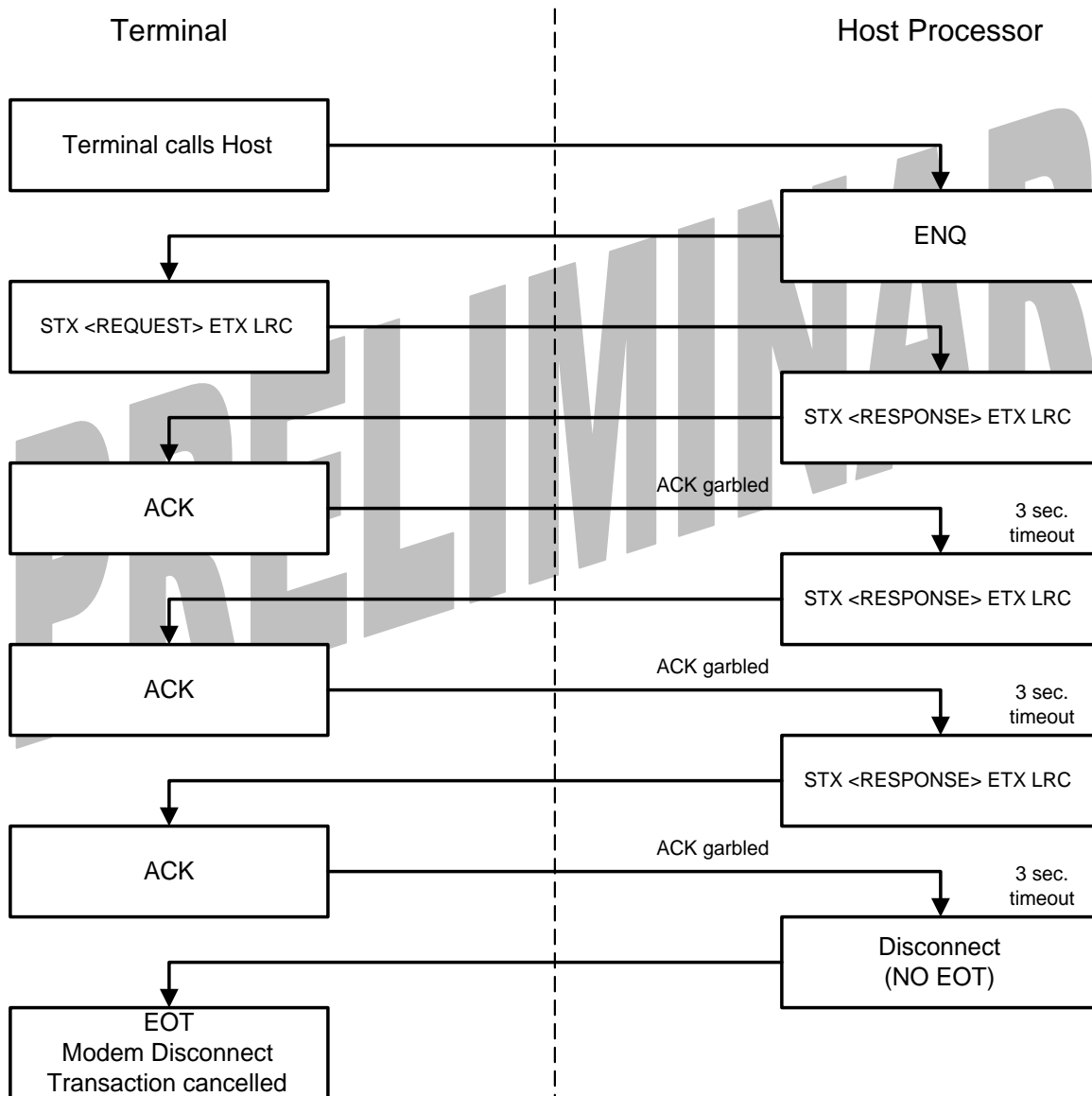
Terminal Does Not Acknowledge Response From Host

This diagram illustrates the line protocol when the terminal does not receive the response properly from the host. In this scenario, the terminal will not dispense the requested amount (if it was approved). The host should reverse the transaction.

Terminal		Host Processor

```
┌──────────────────────┐                          
│  Terminal calls Host  │─────────────────────┐    
└──────────────────────┘                      │    
                                              ▼    
                                    ┌──────────────────────┐
          ┌─────────────────────────│         ENQ          │
          ▼                         └──────────────────────┘
┌──────────────────────┐                                    
│ STX <REQUEST> ETX LRC │────────────────────┐              
└──────────────────────┘                     ▼              
          │            Response lost ◀───┌──────────────────────┐
          ▼                              │ STX <RESPONSE> ETX LRC│
┌──────────────────────┐                 └──────────────────────┘
│ Terminal does not respond │                      │ 3 sec. timeout
└──────────────────────┘                           ▼              
          │            Response lost ◀───┌──────────────────────┐
          ▼                              │ STX <RESPONSE> ETX LRC│
┌──────────────────────┐                 └──────────────────────┘
│ Terminal does not respond │                      │ 3 sec. timeout
└──────────────────────┘                           ▼              
          │            Response lost ◀───┌──────────────────────┐
          ▼                              │ STX <RESPONSE> ETX LRC│
┌──────────────────────┐                 └──────────────────────┘
│ Terminal does not respond │                      │ 3 sec. timeout
└──────────────────────┘                           ▼              
          │            Response lost ◀───┌──────────────────────┐
          ▼                              │     Disconnect        │
┌──────────────────────┐                 │     (No EOT)          │
│      Timeout          │                 └──────────────────────┘
│  Modem disconnect     │                                         
│ Transaction cancelled │                                         
└──────────────────────┘                                         
```
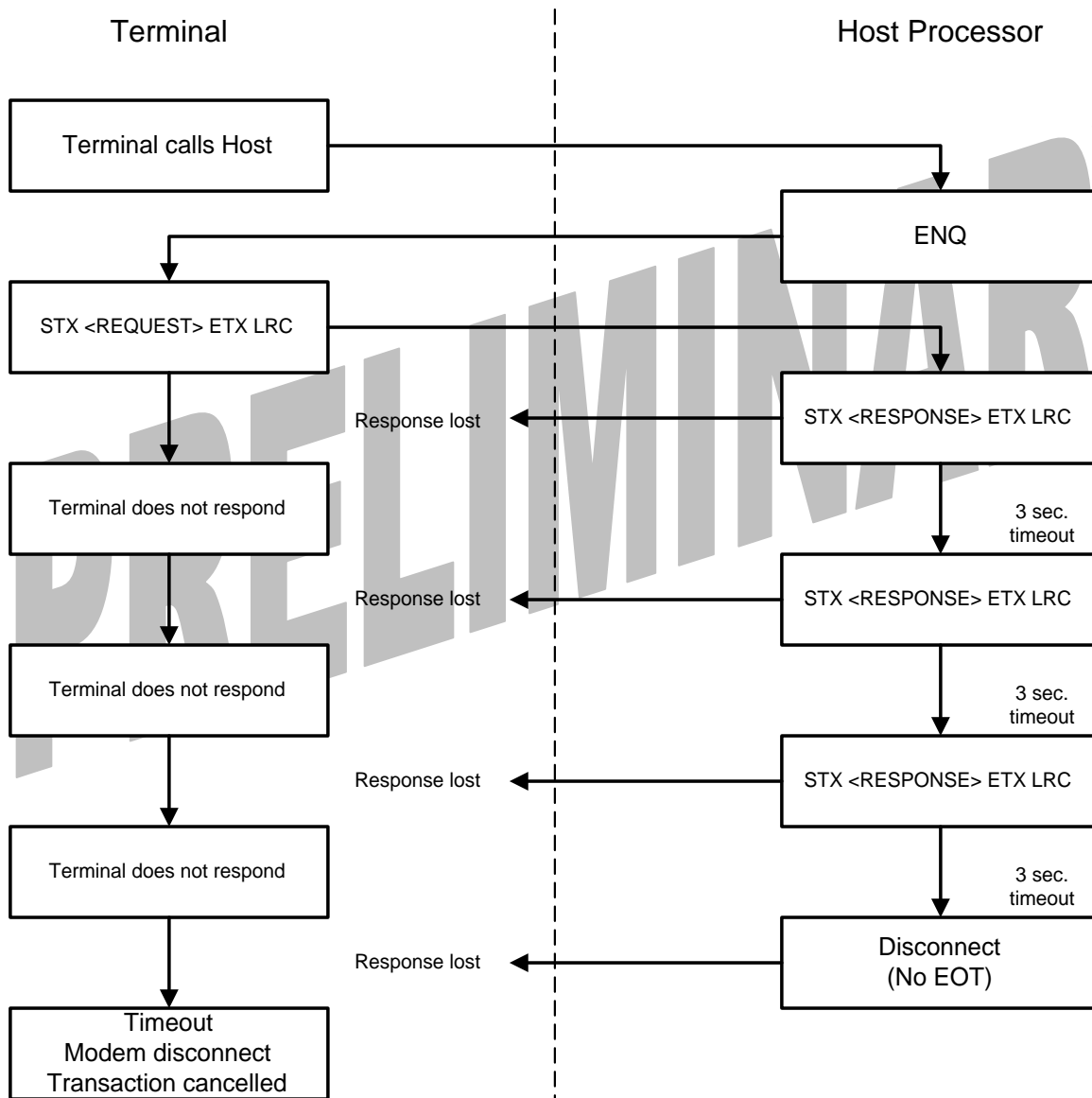
Host Does Not Respond to ACK from Terminal (Default Mode)

This diagram illustrates the line protocol when the host does not respond with an EOT to the ACK from the terminal when operating in default mode (terminal requires Host EOT to dispense). The terminal will not dispense in this scenario.

Terminal

Host Processor

Terminal calls Host

ENQ

STX <REQUEST> ETX LRC

STX <RESPONSE> ETX LRC

ACK

Host does not respond

10 second timeout
Transaction cancelled
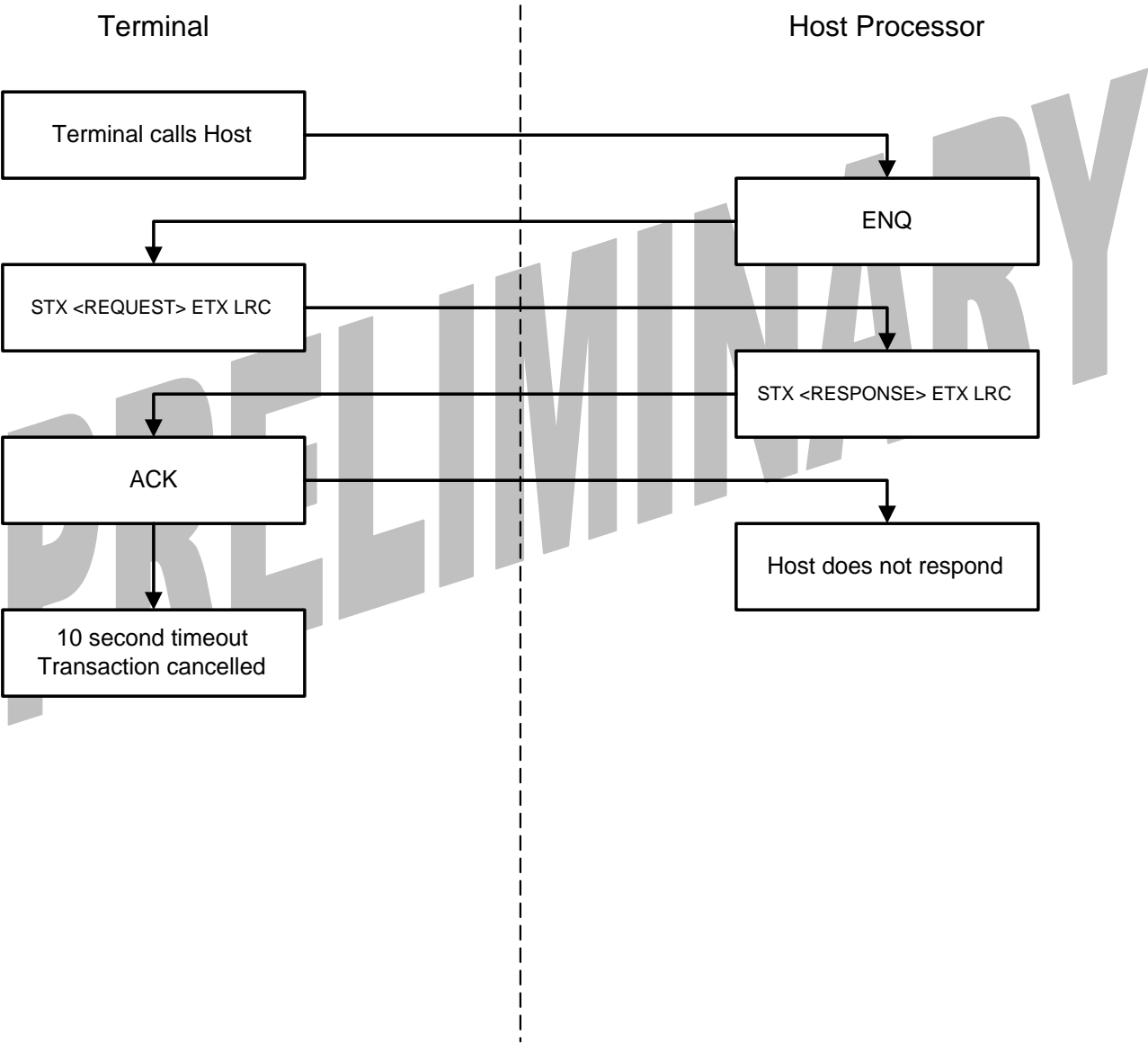
Host Does Not Respond to Request Message

This diagram illustrates the line protocol when the host does not respond to the request message at all. The terminal will not dispense if this happens.

Terminal

Host Processor

Terminal calls Host

ENQ

STX <REQUEST> ETX LRC

| Host does not respond |
| --- |

60 second timeout Transaction cancelled
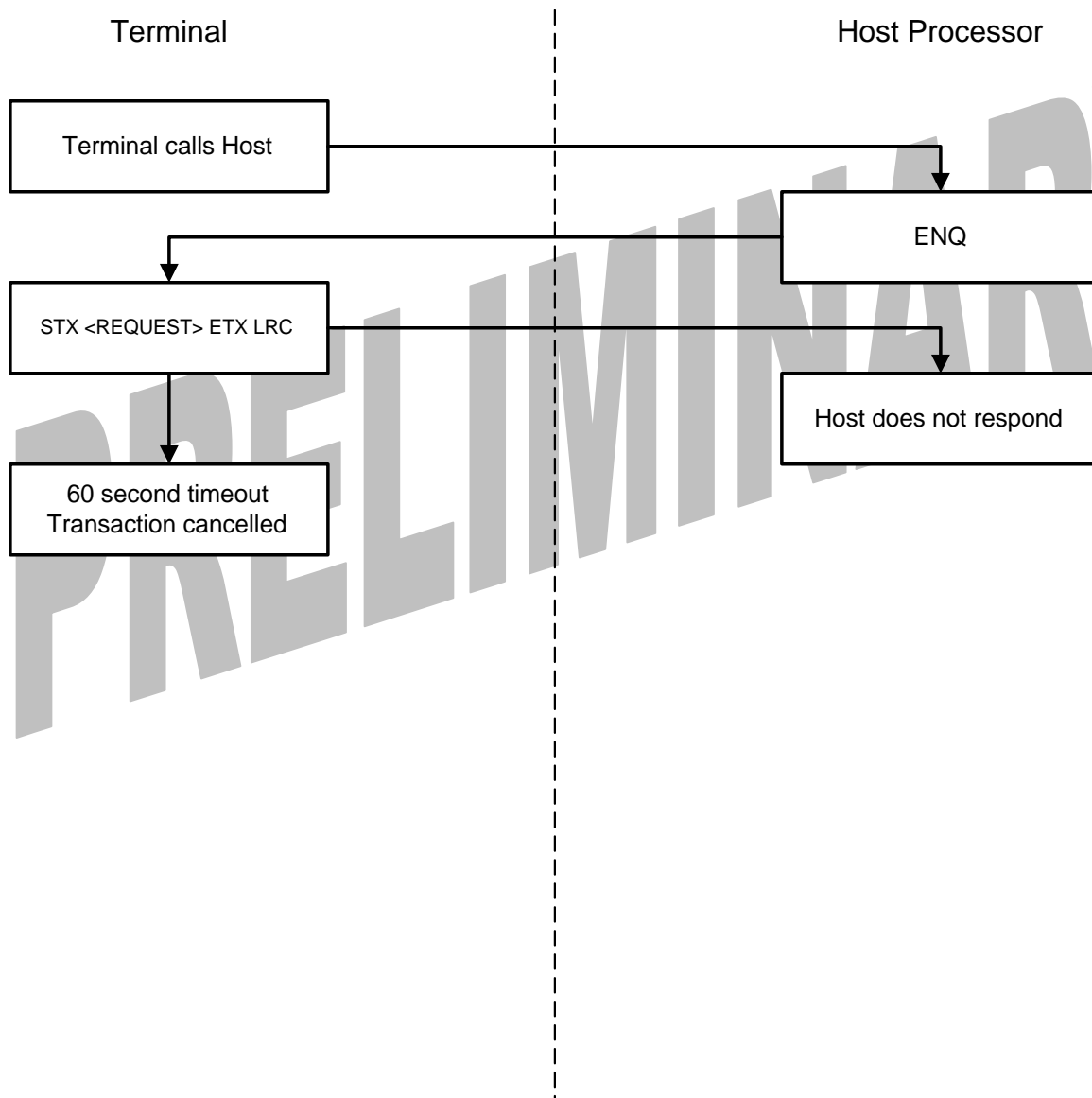
Terminal Does Not Respond to Host ENQ

This diagram illustrates the line protocol when the terminal does not respond to the ENQ character. The host should send at least 4 ENQ characters, one second apart, although this is not required.

Terminal | Host Processor

```
┌─────────────────────┐                    ┌─────────────────────┐
│  Terminal calls Host │───────────────────▶│                     │
└─────────────────────┘                    │         ENQ         │
                                            │                     │
┌─────────────────────┐                    └─────────────────────┘
│ Terminal does not   │◀───────────────────        │
│ respond             │                    ┌─────────────────────┐
└─────────────────────┘                    │         ENQ         │
                                           └─────────────────────┘
┌─────────────────────┐◀───────────────────        │
│ Terminal does not   │                    ┌─────────────────────┐
│ respond             │                    │         ENQ         │
└─────────────────────┘                    └─────────────────────┘
┌─────────────────────┐◀───────────────────        │
│ Terminal does not   │                    ┌─────────────────────┐
│ respond             │                    │         ENQ         │
└─────────────────────┘                    └─────────────────────┘
┌─────────────────────┐◀───────────────────        │
│ Terminal does not   │                    ┌─────────────────────┐
│ respond             │                    │     Disconnect      │
└─────────────────────┘                    └─────────────────────┘
```
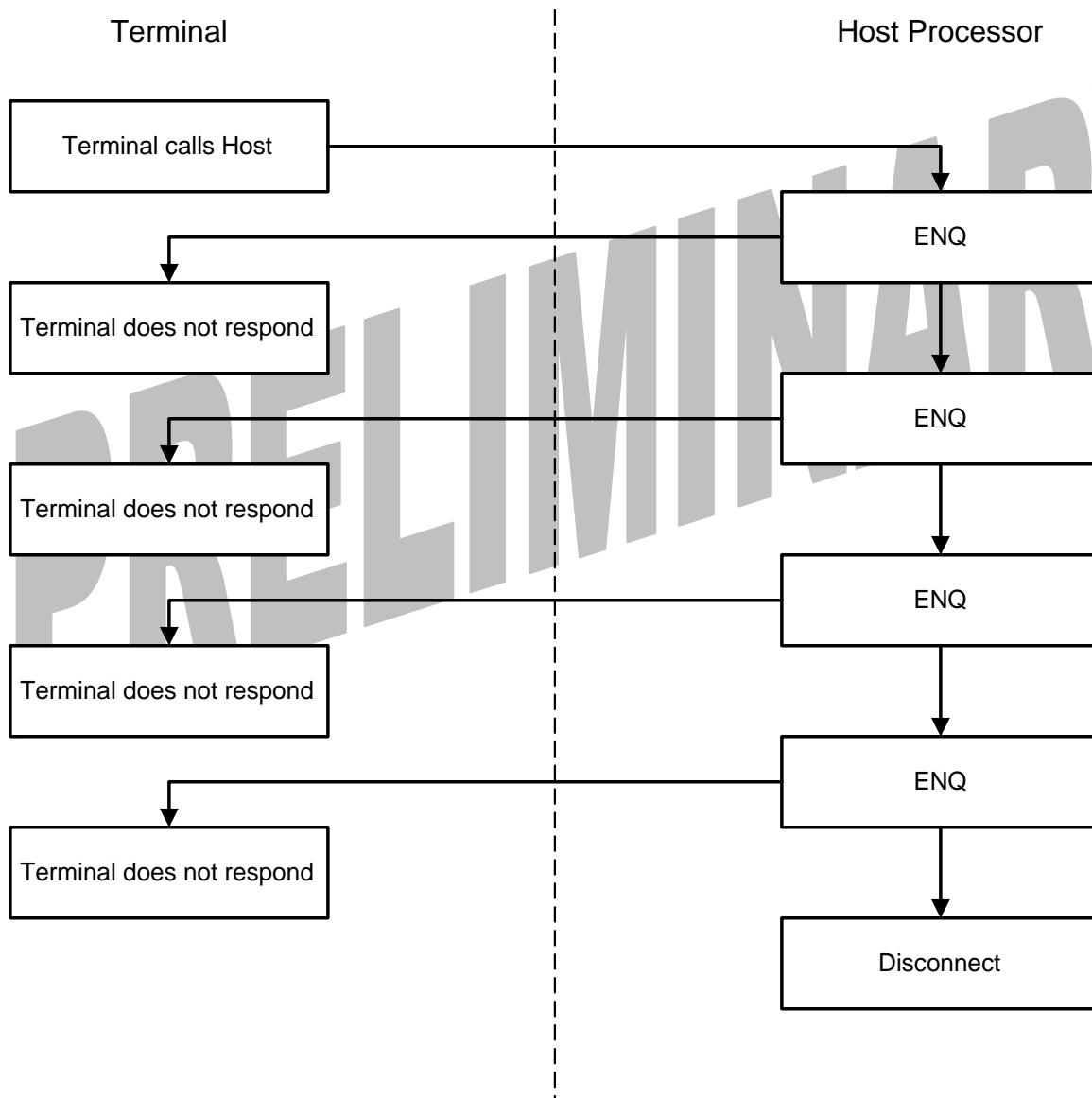
Host Does Not Answer Terminal Call

This diagram illustrates the line protocol when the host does not answer the call. The terminal will try the primary number twice, then the backup number (if programmed) twice. If no answer is received, the transaction will be cancelled.

Terminal	Host Processor

```
┌─────────────────────┐              ┌─────────────────────────┐
│ Terminal calls Host │──────────────│ Host modem does not     │
│ Primary number      │              │ answer or no carrier    │
└─────────────────────┘              │ detected by terminal    │
           │                          │ modem                   │
┌─────────────────────┐              └─────────────────────────┘
│ 30 second timeout.* │
│ Modem disconnects   │
└─────────────────────┘
```

Terminal calls Host
Primary number

30 second timeout.*
Modem disconnects

Host modem does not answer or no carrier detected by terminal modem

3 second delay

Terminal calls Host
Primary number

30 second timeout.*
Modem disconnects

Host modem does not answer or no carrier detected by terminal modem

3 second delay

Terminal calls Host
Backup number

30 second timeout.*
Modem disconnects

Host modem does not answer or no carrier detected by terminal modem

3 second delay

Terminal calls Host
Backup number

30 second timeout.*
Modem disconnects

Host modem does not answer or no carrier detected by terminal modem

* Modem response can shorten timeout

APPENDIX A

ANSI PIN Block Format

This appendix includes two sections from the American National Standards Institute (ANSI) document titled *American National Standard For Personal Identification Number (PIN) Management and Security X.9.8.* This document describes, among other things, the techniques used to secure transmissions of customer PINs over insecure communications pathways. It is presented as a reference only.

3.7.2.2.2 Clear-Text PIN Block Format

The PIN is assumed to consist of 4-12 decimal digits and *shall* be entered by a customer, in sequence as specified by Section 3.5.1.2, with the first digit entered referred to as digit 1 and the last referred to as digit N.

The clear-text PIN format specified *must* be used in interchange and may be used in the terminal to acquirer segment of the network. Bit positions are specified based on numbering the bits in the DEA input block as in Section 3.7.2.2.1.

The clear-text PIN and the customer's account number are constructed as follows:

PIN Block Construction

Bit

1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	65
C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

C -   Control field. Currently, the only defined value is 0000 (binary) which designates the block as containing 4 to 12 four-bit decimal PIN digits representing user-entered characters according to Section 3.5.1.1. Future use of different values of this field could accommodate different character sets.

N -   PIN length entered field. Four-bit binary number with permissible values of 0100 (=4) to 1100 (=12)

P -   PIN digit. Four-bit field having possible values from 0000 to 1001 as defined by Section 3.5.1.1.

F-   Fill digit. Four-bit field having fixed value 1111.

P/F -   PIN digit or fill digit, as determined by PIN length entered field (N).

Account Number Block Construction

Bit

1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	65
0	0	0	0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	

A - The 12-right-most digits of the primary account number (PAN), excluding the check digit. A_1 is the most significant digit and A_{12} is the digit immediately preceding the PAN's check digit.

0 - A decimal pad digit-zero. The first 4-bit fields of the account number block are always padded with this value.

Formatted Clear-Text PIN Block

Next, the PIN and account number blocks are Exclusive OR'd before assembled in the DEA input register.

When the customer's account number is not available, other cryptographic techniques should be used to protect the PIN. Appendix F (ANSI X.9.8) illustrates one such method.

Any network or interchange node having access to the clear-text PIN block (i.e., during a decryption/re-encryption or during a PIN verification) should reject transactions having any of the following:

    a.   Control field value of other than 0000
    b.   A PIN length entered field of value less that 4 or greater that 12
    c.   Any PIN digit from P_1 through P_N of value greater than 9

This serves as a reasonable check on PIN encryption/decryption processing, but does not serve as any indication of validity of the customer-entered PIN.

3.7.2.2.3 Cipher-Text PIN Format

The formatted clear-text PIN block, defined above, then *shall* be encrypted using the DEA on Electronic Code-Book (ECB) mode as shown in Section 3.7.2.2.1. The 64-bit output cipher block is called the reversibly encrypted PIN (or encrypted PIN).

The encrypted PIN *shall* be transmitted between financial institutions as a 64-bit entity in bit oriented communications, as eight 8-bit bytes in 8-bit transparent character oriented communications, as sixteen characters representing hexadecimal digits (0, 1, …, 9, A, B, …, F), or by any other data representation agreed upon by sender and receiver. (Triton Note: The Triton Standard uses 16 hexadecimal digits represented as ASCII characters).

The order of transmission *shall* be for left to right, with respect to the diagram in Section 3.7.2.2.1. For example, in 8-bit transparent communications the first byte transmitted will contain bits 1 though 8 of the DEA output block; the eight byte transmitted will contain bits 57 through 64 of the DEA output block.

APPENDIX B

MAC Protocol Addendum

The MAC fields implemented in this specification follow the ANSI Standard X9.19 format.

The Triple-DES MAC Algorithm implemented in this specification uses "MAC Algorithm 3 - Padding Method 1" as defined in ISO/IEC 9797-1.

This section describes the actual implementation of the fields in the message.
1. Insert a Field ID '^' into one of the miscellaneous fields in the formatted message. Fill this field with 9 ASCII zero characters.
2. Create an 8-byte buffer in RAM called 'INPUT' and fill this block with hex zeroes.
3. Create an 8-byte buffer in RAM called 'OUTPUT' and fill this block with hex zeroes.
4. Begin at the STX character of the formatted message.
5. Take the next 8 ASCII characters from the formatted message (include STX first time through) and transfer them to the INPUT buffer. Use all characters up to and including the ETX. If less than 8 characters are available, pad the remaining position(s) with Binary zeroes.
6. Exclusive-OR the OUTPUT buffer with the INPUT buffer and store in the INPUT buffer.
7. Encrypt the INPUT buffer using DES, or Triple-DES if Triple-DES MAC is enabled and this is the last block(see Figure B1), with the MAC working key(s), MK1 and MK2, and store in the OUTPUT buffer.
8. Repeat steps 5 through 7 until the end of the message is reached (ETX).
9. Discard the right-most 32 bits of the OUTPUT buffer. Convert the remaining 32 bits into ASCII characters, 4 bits at a time to produce 8 ASCII characters.
10. Insert an ASCII space character (20h) after the fourth character.
11. The format of the string should be as follows: 'XXXX<sp>XXXX', where X is a hexadecimal ASCII character (0-F).
12. Insert this 9 character string in place of the 9 ASCII zeroes in the Field ID '^' created in step 1.
13. Calculate the LRC of the message with the MAC field in place.

MAC Field Use
When enabled, the terminal will send the MAC field with all message requests except Configuration Table Download request, and will expect them in all message responses except Configuration Table Download response. If the terminal receives an invalid MAC field in a response message, it will immediately perform a Configuration Table Download on a separate call to update the MAC and/or COMMS key. If the failed MAC was contained in a Transaction Response Message and a withdraw or purchase was performed, a reversal will follow the Configuration Table Download, and if a withdraw was performed, no cash will be dispensed in this case.
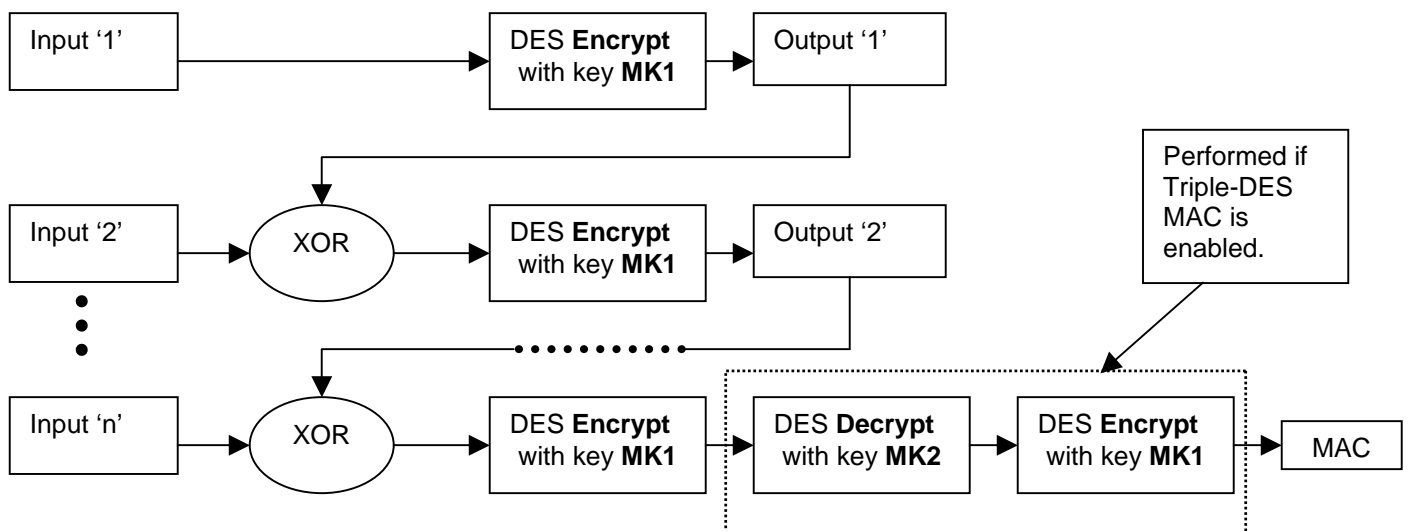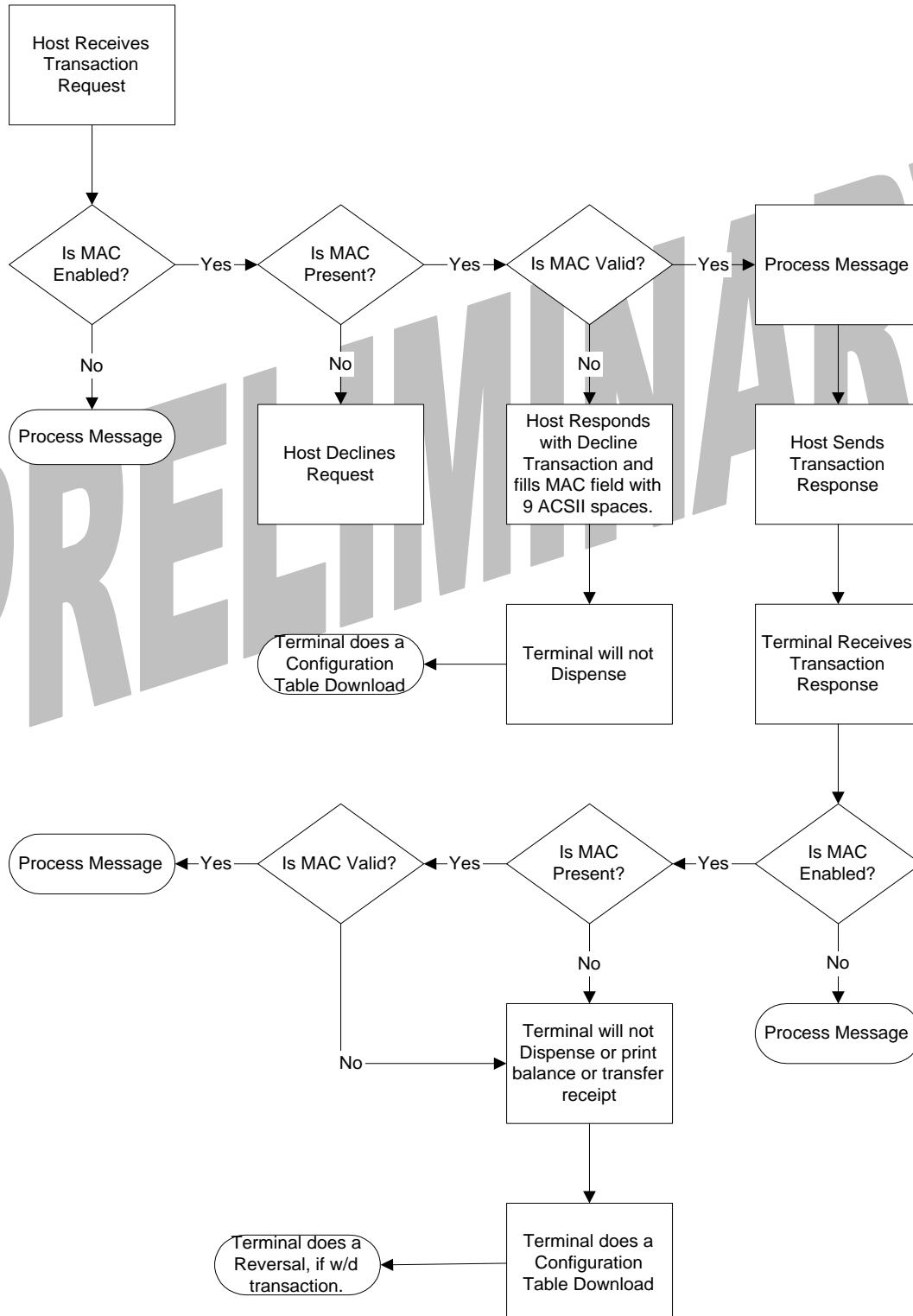

Figure B1 – Triple-DES MAC Algorithm

Message Protocol with MAC Enabled

```
┌─────────────────┐
│ Host Receives   │
│ Transaction     │
│ Request         │
└────────┬────────┘
         │
         ▼
     ◇ Is MAC ◇ ──Yes──► ◇ Is MAC ◇ ──Yes──► ◇ Is MAC Valid? ◇ ──Yes──► ┌──────────────┐
     ◇ Enabled? ◇        ◇ Present? ◇                                    │ Process      │
         │                   │                  │                         │ Message      │
         No                  No                 No                        └──────┬───────┘
         │                   │                  │                                │
         ▼                   ▼                  ▼                                ▼
  ( Process Message )  ┌──────────────┐  ┌──────────────────┐          ┌──────────────┐
                       │ Host Declines│  │ Host Responds    │          │ Host Sends   │
                       │ Request      │  │ with Decline     │          │ Transaction  │
                       └──────────────┘  │ Transaction and  │          │ Response     │
                                         │ fills MAC field  │          └──────┬───────┘
                                         │ with 9 ACSII     │                 │
                                         │ spaces.          │                 ▼
                                         └────────┬─────────┘          ┌──────────────┐
                                                  │                    │ Terminal     │
                                                  ▼                    │ Receives     │
   ( Terminal does a )  ◄──  ┌──────────────┐                          │ Transaction  │
   ( Configuration   )       │ Terminal will│                          │ Response     │
   ( Table Download  )       │ not Dispense │                          └──────┬───────┘
                             └──────────────┘                                 │
                                                                              ▼
```

```
( Process Message ) ◄─Yes─ ◇ Is MAC Valid? ◇ ◄─Yes─ ◇ Is MAC ◇ ◄─Yes─ ◇ Is MAC ◇
                                 │                    ◇ Present? ◇        ◇ Enabled? ◇
                                 │                        │                  │
                                 │                        No                 No
                                 │                        │                  │
                                 │                        ▼                  ▼
                                 │               ┌──────────────┐      ( Process Message )
                                 │               │ Terminal will│
                                 │               │ not Dispense │
                                 No ────────────►│ or print     │
                                                 │ balance or   │
                                                 │ transfer     │
                                                 │ receipt      │
                                                 └──────┬───────┘
                                                        │
                                                        ▼
  ( Terminal does a )  ◄──  ┌──────────────┐
  ( Reversal, if w/d )      │ Terminal does│
  ( transaction.    )       │ a            │
                            │ Configuration│
                            │ Table        │
                            │ Download     │
                            └──────────────┘
```

APPENDIX C

Extended Transaction Code Table †				
CODE	Transaction Type	CODE	Account Type
01	Withdrawal	00	No Account
02	Transfer	11	Primary Checking Bank Account
03	Balance Inquiry	12	Primary Savings Bank Account
04	Prepaid Telephone	15	Primary Credit Card Bank Account
05	Bill Payment	16	Primary Money Market Bank Account
06	Prepaid Electricity	21	Secondary Checking Bank Account
		22	Secondary Savings Bank Account
		25	Secondary Credit Card Bank Account
		26	Secondary Money Market Bank Account
		31	Primary Checking Brokerage Account
		32	Primary Savings Brokerage Account
		35	Primary Credit Card Brokerage Account
		36	Primary Money Market Brokerage Account
		41	Secondary Checking Brokerage Account
		42	Secondary Savings Brokerage Account
		45	Secondary Credit Card Brokerage Account
		46	Secondary Money Market Brokerage Account

To use an extended transaction code string, first place a '99' into the 2-digit transaction code field of the transaction request message. Then construct the extended transaction code string by combining the FID 'l' (ASCII Char - 6Ch) with a transaction type code, a 'from' account type code and a 'to' account type code, consecutively, in the order shown below.

Extended Transaction Code String. – FID 'l' plus Six ASCII numbers. – 'l' + $T_1 T_2 T_3 T_4 T_5 T_6$

$T_1 T_2$ - Transaction Type Code

$T_3 T_4$ - 'From' Account Type Code (Code '00' not allowed)

$T_5 T_6$ - 'To' Account Type Code

The reply transaction codes must match those in the request.

Example:

1.) Transfer from Secondary Money Market Bank Account to Primary Savings Brokerage Account – 'l022632'

† **Preliminary**

APPENDIX D

Triple-DES Encryption of the PIN Block

Triple-DES (3DES) encryption/decryption (as specified in ANSI X9.52) is a sequence of DES encryption/decryption operations as shown in diagram 1 and diagram 2 below. 3DES is highly secure and uses two independent 64-bit block keys, $K1$ and $K2$. Single-DES is less secure and is achieved when $K1$ and $K2$ are equal ($K1 = K2$). $K1$ and $K2$ are obtained by sending both the Encrypted PIN-Key 1 ('~') and Encrypted PIN-Key 2 ('{') FIDS in a response message. The Encrypted PIN-Key's are decrypted using the Master Key, resulting in $K1$ and $K2$. The Clear-Text PIN Block Format and Cipher-Text PIN Format are the same for both Single DES and Triple DES. See APPENDIX A for a description of the PIN Block Format.

The presence of only the Encrypted PIN-Key 1 ('~') in a response message will cause 3DES capable terminals to store $K2$ with the value of $K1$, and set the Encryption Mode Flag (EMF) and the '[' FID to zero (0). The presence of both the Encrypted PIN-Key 1 ('~') and Encrypted PIN-Key 2 ('{') will store $K1$ and $K2$ with separate values and set the EMF and the '[' FID to two (2), **even for equal Key values**. When the Key values are equal ($K1 = K2$) in a 3DES capable terminal, Single-DES encryption/decryption is achieved by performing the 3DES encryption/decryption scheme. Table 1 summarizes the '[' FID and EMF.

| Cleartext PIN block | → | DES **Encrypt** with key **K1** | → | DES **Decrypt** with key **K2** | → | DES **Encrypt** with key **K1** | → | Ciphertext PIN block |
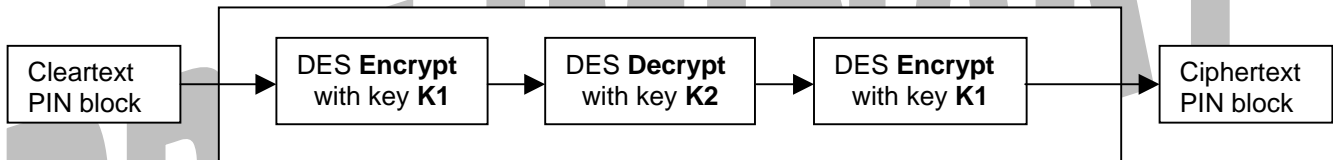
Diagram 1 - 3DES Encryption

| Ciphertext PIN block | → | DES **Decrypt** with key **K1** | → | DES **Encrypt** with key **K2** | → | DES **Decrypt** with key **K1** | → | Cleartext PIN block |
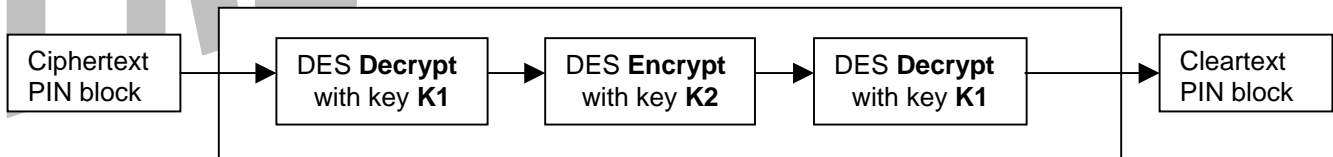
Diagram 2 - 3DES Decryption

	Terminal is 3DES capable		Terminal is not 3DES capable
KEYS received in response message from host	'~' ONLY	'~' & '{'	'~' ONLY
Encryption Mode Flag in Communications header	0	2	0
'[' FID in request message	'[0'	'[2'	NOT SENT

Table 1 – 3DES Capable FID '['

APPENDIX E

Encryption Key Sets

For Triton terminals that support multiple host processors, each host processor is assigned one encryption key set. The terminal parameters for each host processor include, but are not limited to, terminal id number, primary and backup host phone numbers, and master and working encryption keys. An encryption key set consists of three pairs of working keys and three pairs of master keys. Each pair of working keys consists of a left and a right block that is used for either Single-DES or Triple-DES encryption of a PIN-Block, MAC message, or DATA message. The PIN, MAC, and DATA master keys are used for encryption and decryption of the associated PIN, MAC, and DATA working keys. The working keys left and right blocks are decrypted as shown in diagram E2 and diagram E3. The Working keys are transmitted to the terminal in encrypted form by using the appropriate FID as a miscellaneous field in a configuration download message. The Master keys are manually entered or electronically injected at the terminal. The FID's are shown in Table E1.

Configuration parameter	FID
PIN Working Key Left Block	'~'
PIN Working Key Right Block	'{'
MAC Working Key Left Block	'm'
MAC Working Key Right Block	'}'
DATA Working Key Left Block	'ue'
DATA Working Key Right Block	'uf'
PIN Master Key Left Block	
PIN Master Key Right Block	
MAC Master Key Left Block	Manually entered or electronically
MAC Master Key Right Block	injected at the terminal.
DATA Master Key Left Block	
DATA Master Key Right Block	

Table E1 – Service parameters.
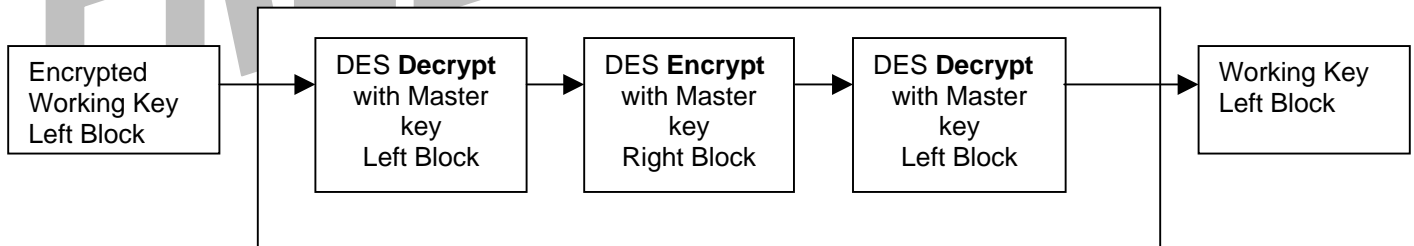
Diagram E2 – Working Key Left Block decryption.
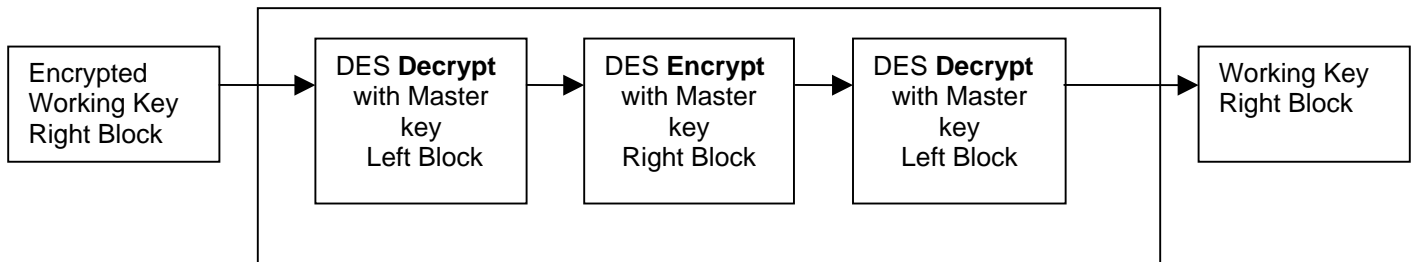
Diagram E3 – Working Key Right Block decryption.

APPENDIX F

ANSI 16-bit CRC

This section describes the implementation of the CRC-16 (ANSI) routine.

1. Insert a FID 'ub' into a miscellaneous field in the message and initialize the 4 ASCII Characters to ASCII zero (0x30) characters.
2. Calculate the CRC on the message excluding the STX, ETX, and LRC (in dial-up).
3. Convert the 2-byte CRC into 4 ASCII characters and insert these in place of the 4 ASCII zeros (0x30) of the message in the order of MSB to LSB.
4. Upon the receipt of the message, the FID 'ub' will be searched for and the 4 ASCII characters representing the CRC-16 value will be extracted and replaced by 4 ASCII zeros (0x30).
5. Recalculate the CRC on the message excluding the STX, ETX, and LRC (in dial-up).
6. Compare calculated CRC with the extracted CRC from the original message.

APPENDIX F

ANSI 16-bit CRC

The following is a C code example of the byte by byte method using a lookup table that considers the data and the final CRC being reflected.

```c
const unsigned int crc_table[256] =
{
0x0000, 0xC0C1, 0xC181, 0x0140, 0xC301, 0x03C0, 0x0280, 0xC241,
0xC601, 0x06C0, 0x0780, 0xC741, 0x0500, 0xC5C1, 0xC481, 0x0440,
0xCC01, 0x0CC0, 0x0D80, 0xCD41, 0x0F00, 0xCFC1, 0xCE81, 0x0E40,
0x0A00, 0xCAC1, 0xCB81, 0x0B40, 0xC901, 0x09C0, 0x0880, 0xC841,
0xD801, 0x18C0, 0x1980, 0xD941, 0x1B00, 0xDBC1, 0xDA81, 0x1A40,
0x1E00, 0xDEC1, 0xDF81, 0x1F40, 0xDD01, 0x1DC0, 0x1C80, 0xDC41,
0x1400, 0xD4C1, 0xD581, 0x1540, 0xD701, 0x17C0, 0x1680, 0xD641,
0xD201, 0x12C0, 0x1380, 0xD341, 0x1100, 0xD1C1, 0xD081, 0x1040,
0xF001, 0x30C0, 0x3180, 0xF141, 0x3300, 0xF3C1, 0xF281, 0x3240,
0x3600, 0xF6C1, 0xF781, 0x3740, 0xF501, 0x35C0, 0x3480, 0xF441,
0x3C00, 0xFCC1, 0xFD81, 0x3D40, 0xFF01, 0x3FC0, 0x3E80, 0xFE41,
0xFA01, 0x3AC0, 0x3B80, 0xFB41, 0x3900, 0xF9C1, 0xF881, 0x3840,
0x2800, 0xE8C1, 0xE981, 0x2940, 0xEB01, 0x2BC0, 0x2A80, 0xEA41,
0xEE01, 0x2EC0, 0x2F80, 0xEF41, 0x2D00, 0xEDC1, 0xEC81, 0x2C40,
0xE401, 0x24C0, 0x2580, 0xE541, 0x2700, 0xE7C1, 0xE681, 0x2640,
0x2200, 0xE2C1, 0xE381, 0x2340, 0xE101, 0x21C0, 0x2080, 0xE041,
0xA001, 0x60C0, 0x6180, 0xA141, 0x6300, 0xA3C1, 0xA281, 0x6240,
0x6600, 0xA6C1, 0xA781, 0x6740, 0xA501, 0x65C0, 0x6480, 0xA441,
0x6C00, 0xACC1, 0xAD81, 0x6D40, 0xAF01, 0x6FC0, 0x6E80, 0xAE41,
0xAA01, 0x6AC0, 0x6B80, 0xAB41, 0x6900, 0xA9C1, 0xA881, 0x6840,
0x7800, 0xB8C1, 0xB981, 0x7940, 0xBB01, 0x7BC0, 0x7A80, 0xBA41,
0xBE01, 0x7EC0, 0x7F80, 0xBF41, 0x7D00, 0xBDC1, 0xBC81, 0x7C40,
0xB401, 0x74C0, 0x7580, 0xB541, 0x7700, 0xB7C1, 0xB681, 0x7640,
0x7200, 0xB2C1, 0xB381, 0x7340, 0xB101, 0x71C0, 0x7080, 0xB041,
0x5000, 0x90C1, 0x9181, 0x5140, 0x9301, 0x53C0, 0x5280, 0x9241,
0x9601, 0x56C0, 0x5780, 0x9741, 0x5500, 0x95C1, 0x9481, 0x5440,
0x9C01, 0x5CC0, 0x5D80, 0x9D41, 0x5F00, 0x9FC1, 0x9E81, 0x5E40,
0x5A00, 0x9AC1, 0x9B81, 0x5B40, 0x9901, 0x59C0, 0x5880, 0x9841,
0x8801, 0x48C0, 0x4980, 0x8941, 0x4B00, 0x8BC1, 0x8A81, 0x4A40,
0x4E00, 0x8EC1, 0x8F81, 0x4F40, 0x8D01, 0x4DC0, 0x4C80, 0x8C41,
0x4400, 0x84C1, 0x8581, 0x4540, 0x8701, 0x47C0, 0x4680, 0x8641,
0x8201, 0x42C0, 0x4380, 0x8341, 0x4100, 0x81C1, 0x8081, 0x4040
};

/* This function will take the pointer to a message (string) and the length of the message
and will return the computed CRC using the crc_table[]. */

unsigned int crc16 (unsigned char *string, int length )
{
    unsigned int crc;
    crc = 0x0000;    /* initial CRC value 0x0000 */
    while (length--)
    {
        crc = ( crc >> 8 ) ^ crc_table[(crc ^ (int) string++) & 0xff];
      /* This performs the modulo-2 division by using the look up table. */
    }
    return(crc); /* return the calculated CRC */
}
```

Appendix G - EMV

Mapping of EMV Data Elements to Existing Fields or FIDS

Some of the data elements required by an issuer to process an EMV transaction map to existing fields or FIDS in the Triton Standard communication protocol. All other fields will be encoded as data in the 'ud' FID as Tag-Length-Value elements or data in the 'uh' FID as TSEMVID-Length-Value elements. However, these EMV data elements that have functionally equivalent fields or FIDS will instead continue to be transported as such, instead of being data in the 'ud' or 'uh' FIDs. The following table shows which EMV data elements can be found in which existing fields or FIDS.

EMV Field	Tag	Existing Field or FID
Amount Authorized	9F02	Standard Amount 1 field or 'e' FID data
Amount Other	9F03	No field or FID. Always implied to be 0.
Enciphered PIN	99	PIN Block
Track 2 Equiv. Data	57	Track 2 field
Transaction Seq. Counter	9F41	Sequence Number field (only if not present in the 'ud' FID)†Sequence Number field
Terminal ID	9F1C	Terminal ID field

Table EMV-1.1.1

† Please note that if the EMV Transaction Sequence Counter tag (9F41) appears in the 'ud' FID, the value found in that FID is the definitive tag 9F41. In such a case, the sequence number found in the Triton Standard Sequence Number message field is not the EMV Transaction Sequence Counter tag (9F41). Instead, the EMV Transaction Sequence Counter holds a separate, EMV-compliant sequence number, incremented only for EMV transactions, while the Triton Standard Sequence Number field holds the usual sequence number, incremented for every transaction. These two sequence counters will almost always have different values.

Please note that if EMV data is sent from the terminal in a transaction request message in the 'ud' FID, the transaction response message must contain a 'ud' FID with, at minimum, tag 8A for the transaction to be approved.

Encoding of Other EMV Data Elements

Other EMV data elements present in a message will be encoded into the 'ud' or 'uh' FIDs. Data elements specified in the EMV standard that are assigned unique tags will be packed into the 'ud' FID (Encoded EMV data block). Data elements specified in the EMV standard but not assigned a tag will be packed into the 'uh' FID (Encoded EMV untagged-data block).

Encoded EMV data block ('ud' FID)

The data that follows the 'ud' FID is of variable length and contains zero or more data elements encoded according to Basic Encoding Rules—Tag-Length-Value (BER-TLV). See ISO/IEC 8825:1990, ISO/IEC 7816-4:1995 Annex D, and EMV 2000 Book 3 Annex B for a more complete and official description of this format. Information presented here is a summary of important points from these documents and is included for convenience only.

Encoded EMV untagged-data block ('uh' FID)

The data that follows the 'uh' FID is of variable length and contains zero or more data elements encoded according to a scheme identical to the Basic Encoding Rules—Tag-Length-Value (BER-TLV) scheme. However, the identifiers (TSEMVIDs) used in this scheme (instead of tags) are proprietary to Triton's communication specification. **Note**: It is important for any host processing this block to extract these data elements before sending them anywhere. The TSEMVIDs are not specified in the EMV standard and are not meaningful anywhere outside of the Triton Standard communication scheme. See table EMV-1.1.2 for a listing of these TSEMVIDs. TSEMVIDs are encoded using the same rules that cover the encoding of the tag field in BER-TLV.

Appendix G - EMV

Assigned TSEMVID	Data Element in EMV Standard
DF01	Certification Authority Public Key Check Sum
DF02	Certification Authority Public Key Exponent
DF03	Certification Authority Public Key Modulus
DF04	Default Dynamic Data Authentication Data Object List (DDOL)
DF05	Issuer Script Results
DF06	Last Online ATC Register
DF07	Maximum Target Percentage to be used for Biased Random Selection
DF08	Merchant Name and Location
DF09	Message Type
DF0A	Personal Identification Number (PIN) Pad Secret Key
DF0B	Target Percentage to be used for Random Selection
DF0C	Terminal Action Code - Default
DF0D	Terminal Action Code - Denial
DF0E	Terminal Action Code - Online
DF0F	Threshold Value for Biased Random Selection
DF10	Transaction Reference Currency Code
DF11	Default Transaction Certificate Data Object List (TDOL)

Table EMV-1.1.2

Basic Format

BER-TLV data elements are each represented with three fields, a tag, a length, and a value. The tag field uniquely identifies the data element. The length field specifies the length in bytes of the value field. The value field holds the actual data element bytes. The following description of these fields apply *before* encoding as 7-bit ASCII hex digits for packing into a Triton communication message.

Tag

For the purposes of this specification, tag fields will always be one or two bytes, although they are not restricted to such by ISO/IEC 8825:1990. Values 0x00 and 0xFF are not considered valid tags, as per ISO/IEC 7816-4. Tags code a Class, Type, and Number; see table B-1 in Annex B of EMV 2000 Book 3 for the coding scheme of a tag. As shown in the table, if the least significant 5 bits of the first byte of the tag are 1, the tag is a two-byte tag. Otherwise, it is a one-byte tag.

Defined tags also carry with them an implied format of the encapsulated data element. See EMV 2000 Book 3 Annex A for a table of defined tags and associated data formats defined by EMV, as well as documentation for individual payment systems that may define their own, issuer-specific tags.

Length

For the purposes of this specification, length fields will always be one, two, or three bytes, although they are not restricted to such by ISO/IEC 8825:1990. The length field specifies the length in bytes of the following value field. Lengths of 0x00 are allowed and indicate the absence of a value field.

If the most significant bit of the most significant byte of the length field is 0, the length field is one byte and the remaining seven bits encode the length value (0-127). If the most significant bit of the most significant byte is 1, the length field is more than one byte and the remaining seven bits encode the number of bytes that follow the most significant in the length field. The subsequent bytes together represent an integer that specifies the length in bytes of the value field.

Value

The value field consists of zero or more data bytes as specified in number by the length field. These bytes represent the actual data of the data element.

Appendix G - EMV

Packing of TLV Encoded Data Elements in the 'ud' FID
TLV encoded data elements will be packed into the data of the 'ud' FID with no separation. All bytes of TLV encoded data elements, when packed into the data of the 'ud' FID, will be represented as ASCII encoded hexadecimal digits, requiring two digits to represent a byte, effectively doubling the size of the data. This is necessary to keep message formatting characters, such as the field separator (0x1C) and end of text (0x03) from being included in the 'ud' FID data. The length field of the TLV encoded data elements will reflect the size of the value field before it is encoded into ASCII hex digits so care must be taken in parsing the elements. Several examples follow for clarity.

Packing of Untagged Data Elements in the 'uh' FID
Untagged data elements defined in the EMV standard, encoded using a TSEMVID, length, and value, will be packed into the data of the 'uh' FID with no separation. All bytes of the encoded data elements, when packed into the data of the 'uh' FID, will be represented as ASCII encoded hexadecimal digits, requiring two digits to represent a byte, effectively doubling the size of the data. This is necessary to keep message formatting characters, such as the field separator (0x1C) and end of text (0x03) from being included in the 'uh' FID data. The length field of the encoded data elements will reflect the size of the value field before it is encoded into ASCII hex digits so care must be taken in parsing the elements.

EMV Example 1

A basic example with one-byte lengths is presented here.

Tag	Length	Data Bytes									
82	2	0x1C	0x00								
9F26	8	0xF4	0x7A	0x21	0xE3	0x9C	0xAF	0x5D	0x07		

Table EMV-2.1.1

Resulting Bytes in the 'ud' FID Data								
0x38 ('8')	0x32 ('2')	0x30 ('0')	0x32 ('2')	0x31 ('1')	0x67 ('C')	0x30 ('0')	0x30 ('0')	0x39 ('9')
0x46 ('F')	0x32 ('2')	0x36 ('6')	0x30 ('0')	0x38 ('8')	0x46 ('F')	0x34 ('4')	0x37 ('7')	0x41 ('A')
0x32 ('2')	0x31 ('1')	0x45 ('E')	0x33 ('3')	0x39 ('9')	0x43 ('C')	0x41 ('A')	0x46 ('F')	0x35 ('5')
0x44 ('D')	0x30 ('0')	0x37 ('7')						

Table EMV-2.1.2

EMV Example 2

A more complicated example with a three-byte length is shown here. Note the encoding of the length 289 as 0x820121, forming three bytes 0x82, 0x01, and 0x21, yielding the eight hex digits 0x38, 0x32, 0x30, 0x31, 0x32, and 0x31. The first and most significant byte, in binary, is *10000010$_b$*, meaning that this length is a multi-byte length field (most significant bit is 1) and there are two bytes following in the length field (remaining bits code the number 2). The remaining bytes, 0x01, and 0x21 code the number of bytes in the value field by forming the number 0x121 in hex, or 289 in decimal.

Tag	Length	Data Bytes									
91	10	0x84	0xB6	0xDE	0xAD	0xF0	0x0F	0x0A	0x11	0x9C	0x00
8E	289	Data bytes not shown…									

Table EMV-2.2.1

Resulting Bytes in the 'ud' FID Data								
0x39 ('9')	0x31 ('1')	0x31 ('0')	0x30 ('A')	0x38 ('8')	0x34 ('4')	0x42 ('B')	0x36 ('6')	0x44 ('D')
0x45 ('E')	0x41 ('A')	0x44 ('D')	0x46 ('F')	0x30 ('0')	0x30 ('0')	0x46 ('F')	0x30 ('0')	0x41 ('A')
0x31 ('1')	0x31 ('1')	0x39 ('9')	0x67 ('C')	0x30 ('0')	0x30 ('0')	0x38 ('8')	0x45 ('E')	0x38 ('8')
0x32 ('2')	0x30 ('0')	0x31 ('1')	0x32 ('2')	0x31 ('1')		Data bytes not shown…		

Table EMV-2.2.2

Appendix G - EMV

EMV Elements to be Included in Messages

While, theoretically, any EMV data element may be sent or received to process an EMV transaction, hosts should typically expect certain common fields to be included in transaction requests, transaction responses, and transaction reversals. These common fields are listed here. This is by no means an exhaustive list of all possible EMV data elements that can appear in messages, so hosts should be prepared for any defined EMV tag. Any tag not available to the terminal may not be sent, so hosts should be prepared to handle missing data.

Common Transaction Request Fields

Field Description	Tag	TSEMVID	Existing Field or FID	Notes
Amount Authorized	-	-	Amount 1 or 'e' FID	Use Amount 1 field if not using extended amounts, 'e' FID otherwise.
Application ID	9F06 or 4F	-	-	
App Interchange Profile	82	-	-	
App Transaction Counter	9F36	-	-	
Cryptogram	9F26	-	-	
Cryptogram Info Data	9F27	-	-	
Enciphered PIN	-	-	PIN Block	
Issuer App Data	9F10	-	-	
Issuer Script Identifier	9F18	-	-	Only if previous trans. had a script.
Issuer Script Results	-	DF05	-	Only if previous trans. had a script.
Terminal Verification Results	95	-	-	
Unpredictable #	9F37	-	-	
App PAN Seq. #	5F34	-	-	
Terminal ID	-	-	Term. ID Field	
Terminal Country Code	9F1A	-	-	
Track 2 Equiv. Data	-	-	Track 2 Field	
Transaction Currency Code	5F2A	-	-	
Transaction Date	9A	-	-	
Transaction Type	9C	-	-	
Transaction Seq. Counter	9F41	-	or Seq. Number Field	If the 9F41 tag appears in the 'ud' FID, it contains a separate, EMV-compliant sequence number incremented only for EMV transactions. In this case, the Triton Standard Sequence Number field contains the usual sequence number, incremented for every transaction.
IFD Serial Number	9F1E	-	-	
Terminal Capabilities Profile	9F33	-	-	
Terminal Type	9F35	-	-	
CVM List	8E	-	-	
CVM Results	9F34	-	-	
POS Entry Mode	9F39	-	-	
Transaction Status Information	9B	-	-	

Table EMV-3

Common Transaction Response Fields

Field Description	Tag	TSEMVID	Existing Field or FID	Notes
Authorization Response Code	8A	-	-	This tag is required for a successful transaction. A value of '00' indicates a request for an approval from the ICC, while any other value indicates a request for a decline from the ICC.
Authorization Code	89	-	-	
Issuer Authentication Data	91	-	-	
Issuer Script	71	-	-	
Issuer Script	72	-	-	
Issuer Script Identifier	9F18	-	-	

Table EMV-4

Appendix G - EMV

Common Reversal Fields

Field Description	Tag	TSEMVID	Existing Field or FID	Notes
Application ID	9F06 or 4F	-	-	
App Interchange Profile	82	-	-	
App Transaction Counter	9F36	-	-	
Issuer App Data	9F10	-	-	
Terminal Verification Results	95	-	-	
Amount Authorized	-	-	Amount 1 or 'e' FID	Use Amount 1 field if not using extended amounts, 'e' FID otherwise.
App PAN Seq. #	5F34	-	-	
Terminal ID	-	-	Term. ID Field	
Track 2 Equiv. Data	-	-	Track 2 Field	
Transaction Type	9C	-	-	
Transaction Seq. Counter	9F41	-	or Seq. Number Field	If the 9F41 tag appears in the 'ud' FID, it contains a separate, EMV-compliant sequence number incremented only for EMV transactions. In this case, the Triton Standard Sequence Number field contains the usual sequence number, incremented for every transaction.
Issuer Script Identifier	9F18	-	-	
Issuer Script Results	-	DF05	-	
Transaction Status Information	9B	-	-	

Table EMV-5

Issuer Script Results

The results of Issuer Scripts, after execution, will be sent at one of two possible times. If the transaction that contained the issuer scripts requires a reversal, during that reversal, the results will be sent (TSEMVID DF05). However, if that transaction did not require a reversal, the script results will be sent during the next transaction request message.

Issuer script results are encoded as detailed in the EMV specification, book 4, Annex A5.

Appendix H – Top Up

E*Trade, Triton Waves, United Kingdom, and South Africa versions of terminal software support mobile phone top-up transactions. Each version requires a different mix of miscellaneous FIDs for proper operation. Table H1 shows the proper FIDs to use for each version. See the Valid Miscellaneous Field ID Table for the proper message type to place the FID into.

FID and description	E*Trade Transaction Code 44		Triton Waves Transaction Code 44		United Kingdom Transaction Code 44		South Africa Transaction Code 99 Use Extended Transaction Code String. – FID 'l'	
	Request	Response	Request	Response	Request	Response	Request	Response
xa Telco-product Serial Number						X		
xb mobile phone number	X		X	X activation phone number	X		X	
xd general taxes		X	X	X				
xe top-up transaction totals and amounts	X	X	X	X				
xf contact phone number		X		X		X		X
xg service provider name		X	X	X	X	X	X	
xh Expiration date		X						
xn Actual amount debited from the customer's account								X
xp voucher PIN number				X				X
xq service provider name and fast cash amounts				X		X and service provider ID		
xt general tax rate				X				
xu service provider ID					X			
xv service provider transaction totals and amounts					X	X		

Table H1 – Top Up FIDs