Poynt EMV Configuration Specification

(Revision 0.24)

09/29/2020

Table of Contents

1. Overview

Poynt Card reader EMV configurations can be read and update using PoyntConfigurationService. Poynt Services loads the EMV configurations for a given terminal based on the merchant acquirer from the cloud at the time of device activation and also during runtime as needed or requested by the acquirer.

All applications that need the EMV Configuration parameters can utilize the PoyntConfigurationService on the terminal to retrieve what they are looking for.

Poynt EMV Configuration is separated into 4 distinct data elements.

1. Terminal Configuration
2. AID Configuration
3. CA Public key Configuration
4. Revocation list Configuration
5. Exception list Configuration

2. Terminal Configuration

The Poynt Configuration service maintains three separate Terminal Configurations, one each for contact, contactless and MSR card interfaces. A terminal configuration for a card interface applies to all card applications (AIDs) supported by the Reader for that card interface.

When a Card Reader powers up for the first time, it is assumed to have no terminal configurations. In this case the Reader will itself set a default terminal configuration for each card interface based on the defaults defined in it's corresponding firmware. Once the initial default terminal configurations are set for each card interface, the Reader should not automatically set or change the terminal configuration unless new configuration has been loaded through Poynt Configuration service.

The terminal configuration applies to all card applications, regardless of the AID.

When the Reader receives this command, it should use the "mode" to determine whether the config should be modified or overwritten. Possible values of the Mode field are
00: Modify
01: Overwrite

If the Mode is set to "Modify", the Reader should not delete the existing terminal configuration for the specified interface but will perform a non-destructive modification of the configuration. If a tag already exists in the existing terminal configuration, the Reader should just modify the length and value. If a tag is not present in the existing terminal configuration, the Reader should append the new TLV.

If the Mode is set to “Overwrite” then it should delete the entire existing terminal configuration for the specified card interface and overwrite it with the configuration TLVs specified in the command data. Before deleting the existing configuration, it should make sure that the command data does not contain any mall formatted TLVs.

Format of the Command Data is given in the following Tables.

2.1 Request Data Format Common to all configuration Interfaces

Parameter	Data Item & Description	Format	Length (in Bytes)
mode	Mode The Mode field is used to indicate whether to modify the configuration or to perform a destructive overwrite of the configuration. Possible values of the Mode field are 00: Modify 01: Overwrite 02: Reserved (Not Applicable to Terminal Config) Presence: Mandatory. Applies to: CT, CL, MSR	b	Field Len: 1
- cardInterface	Card Interface Indicates the card interface for which to set the terminal configuration. The format of this byte is given below. Bit 0: MSR Terminal Configuration. Bit 1: Contactless Terminal Configuration. Bit 2: Contact Terminal Configuration. Bits 3-7: RFU. The RFU bits must be set to 0. Only one of the defined bits can be set at a time. Therefore this can have one of three values: 01h = MSR Terminal Configuration 02h = Contactless Terminal Configuration 04h = Contact Terminal Configuration Presence: Mandatory. Applies to: CT, CL, MSR	b	Field Len: 1
data	The first two fields (Mode and Card Interface), will be followed by the Terminal Configuration data items for Contactless, Contact or MSR interface. Each data item will be formatted as a TLV object. The TLV data items that are included in the Terminal Configuration for each card interface are given in the tables that follow.		

2.2 Terminal Configuration Data Items for the Contact Interface

Tag	Data Item & Description	Format	Length (in Bytes)
5F2A	Transaction Currency Code For CT this is supposed to be an AID item but adding it here since it is defined as a Terminal parameter by some CT EMV Kernels and makes better sense.	n3	2
5F36	Transaction Currency Exponent	n1	1
5F57	Account Type	n2	1
97	Default TDOL This value of TDOL is used if the card does not provide a TDOL. This is an AID configuration data item but is being defined here as a Terminal parameter as well since the CT EMV Kernel uses it as Terminal Config. Note: As per EMV Spec 97 is the tag for TDOL (Card-resident) but we are using it for Terminal-resident Default TDOL as well. The Kernel will first look for TDOL in the Card Tag List and if it does not find it there it will look in the Terminal Tag List.	b	Variable
9C	Transaction Type	n2	1
9F1A	Terminal Country Code	n3	2
9F1B	Terminal Floor Limit	b	4
9F1C	Terminal ID	8	an 8
9F1E	Interface Device (IFD) Serial Number	8	an 8
9F33	Terminal Capabilities	b	3
9F35	Terminal Type	n2	1
9F40	Additional Terminal Capabilities	b	5
9F41	Transaction Sequence Counter	n4-8	2-4
9F49	Default DDOL This value of DDOL is used if the card does not provide a DDOL. This is an AID configuration data item but is being defined here as a Terminal parameter as well since the CT EMV Kernel uses it as Terminal Config. Note: As per EMV Spec 9F49 is the tag for DDOL (Card-resident) but we are using it for Terminal-resident Default DDOL as well. The Kernel will first look for DDOL in the Card Tag List and if it does not find it there it will look in the Terminal Tag List.	b	Variable
E013	Target Percentage to be used for Random Selection	b	4
E014	Maximum Target Percentage to be used for Biased Random Selection	b	4
E015	Threshold Value for Biased Random Selection	b	4
EF50	Decline without performing Terminal Action Analysis if online communication is unsuccessful.	b	1
DFD6 ~~1F810F~~	Advice Supported	b	1
1F8110	Force Terminal Risk Management (Credit Call EF40)	b	1
1F8111	Recommended CDA Processing (Credit Call EF49)	b	4

Tag	Data Item & Description	Format	Length (in Bytes)
1F8112	Decline on Comms Fail (Credit Call EF50)	b	1
1F8114	PIN Bypass Supported Possible Values: 00h: PIN Bypass not supported. 01h: PIN Bypass supported Whether PIN Bypass is supported or not, how the PIN Entry UI (Enter Button, Cancel Button, Timeout) behave is defined by *PIN Entry UI Config* (Tag 1F8171). Note: This parameter is a Reader parameter and should be set to the same value in each terminal configuration (CT, CL, MSR). If this tag is missing from the terminal configuration for a particular interface, then the Reader may get the value from the terminal configuration of one of the other two interfaces.	b	1
1F8171	PIN Entry UI Config Indicates how the PIN Entry UI should behave. Possible Values: 01h: Behavior 1 - PIN Bypass on Cancel Button (Default) 02h: Behavior 2 - PIN Bypass on Enter Button (If No PIN Entered) For more detailed information on PIN Entry UI Behavior see *`Appendix A.4 PIN Entry UI Configuration Behaviors*. Note: This parameter is a Reader parameter and should be set to the same value in each terminal configuration (CT, CL, MSR). If this tag is missing from the terminal configuration for a particular interface, then the Reader may get the value from the terminal configuration of one of the other two interfaces.	b	1
1F8220	Terminal Behavior on Missing PIN Key Indicates how the Terminal should behave if the PIN Encryption Key is missing. Applies to Online PIN encryption key only. Possible Values: 01h: Terminate Transaction on Missing PIN Key (Default) 02h: Continue Transaction on Missing PIN Key and treat This situation as “PIN Entry Required and PIN Pad Not Present or PIN Pad Not Working”	b	1
1F8226	Terminal Behavior on PIN Entry Timeout Indicates how the Terminal should behave if there was a PIN Entry Timeout (overall or inter-digit timeout). Applies to both Online and Offline PIN entry. Possible Values: 00h: Treat it as “PIN Pad not working” and continue the Transaction (Default) 01h: Treat it as an attempted PIN Bypass. Terminal behavior will depend on whether PIN Bypass is supported or not. Presence: Optional	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
1F8230	Enable/Disable RNIB related features for ADA PIN entry. Possible Values 00h: RNIB features disabled 01h: RNIB features enabled RNIB specific features include - Firmware will send *ADA Swiped* notifications during ADA PIN entry after ADA button has been swiped. - Firmware will NOT beep after ADA PIN digit entry double tap. The beep will be handled by Android - Inter-digit time out would be 3 minutes instead of 1 minute - ADA digit input requires double tap after swipe instead of single tap - ADA input swipe criteria reduced i.e. shorter ADA swipes accepted as valid.	b	1
1F8122	CT to MSR Fallback Configuration This data item allows configuration of Contact (Chip) to MSR fallback based on EMV, various card association, acquirer or regional (L3) rules. The format of this data item is as follows: Byte 1: Disable “Contact (Chip) Card to MSR Fallback” By default, “Contact to MSR fallback” is supported. However, this data item can be used to disable support for this feature. Possible Values 00h: Contact Card to MSR Fallback supported. This is the default if this data item is not present. 01h: Disable “Contact Card to MSR Fallback” support. If CT to MSR fallback is supported, then the standard method for fallback specified by EMV will always be supported. However, support for non-standard fallback methods can be configured via Byte 2. Byte 2: Non-EMV Fallback Methods Supported. This byte can be used to configure only the non-standard fallback methods that are usually outside the scope of EMV and are usually specified by the card associations, acquirers or regional rules. The format of this byte is as follows. Bit 7: Enable Fallback on Empty Candidate List Bit 6: Enable Fallback on Card Blocked Bit 5: Enable Fallback on App Blocked Bit 4: Enable Fallback on Chip Read Error during App Sel Bit 3: Enable Fallback on Chip Read Error during GPO Bit 2: Enable Fallback on Chip Read Error during Read Recs Bit 1: Enable Fallback on Chip Read Error during Gen AC 1 Bit 0: Enable Fallback on Chip Read Error During Gen AC 2 Byte 3: RFU (must always be set to 00h)	b	3

Tag	Data Item & Description	Format	Length (in Bytes)
1F8123	Allow MSR transaction on Chip Card (without Fallback) As per EMV, if a dual card (Chip + MSR) is swiped the Reader is supposed to perform a Contact EMV transaction and not an MSR transaction. The only condition under which an MSR swipe transaction is allowed is a fallback condition. By default, this is the behavior of the Reader. This data item can be used to override this EMV restriction and allow an MSR transaction even though a dual card (Chip + MSR) is swiped. Possible Values 00h: Do not allow MSR transaction on chip card without a fallback condition. This option complies with the CT EMV specification. This will be the default behavior if this data item is missing. 01h: Allow MSR transaction on chip card without a fallback condition (which is non-compliant to EMV). Important Note: Setting this data item to 01h will violate the EMV specification and hence result in the Reader becoming non-compliant to Contact EMV L2. This option should only be used in markets where EMV is not a requirement or in markets that are in transition from MSR to EMV (provided it is permitted by the relevant stake holders).	b	1
1F812E	Stop after read record Flow Timeout The time in seconds that the Reader will wait for the Terminal to calculate the adjusted amount and send a "*Continue Transaction after stop after read record Flow*" or "*Cancel*" command after indicating to the Terminal that stop after read record flow is required. The timeout value may range from 1 to 300 seconds. This field is used only if stop after read records special flow for amount adjustment is requested. **Important:** For PCI compliance, the value of this timeout MUST be limited to 300 seconds (i.e. 5 minutes) or less, and the firmware MUST enforce this limit	b	2
1F8130	Terminal Supported Languages The list of languages supported by the Terminal. Each language in this list is represented by 2 alphabetical characters as defined in ISO 639. For example, in the following TLV definition 1F81300C656E707466727A6872756573 The parsed data is as follows: 656E = "en" = English 7074 = "pt" = Portuguese 6672 = "fr" = French 7A68 = "zh" = Chinese 7275 = "ru" = Russian 6573 = es = Spanish Note: From the terminal side the language code must always be in lower case letters, however, the Reader should accept both lower and upper case codes. See Appendices for Overview of Multi-Language Support.	an2	Variable

Tag	Data Item & Description	Format	Length (in Bytes)
1F8131	Configuration Version Version of the terminal configuration for the contact interface. This is an optional field and can be used to store a version or a configuration identifier. The actual contents or format of this field are out of the scope of this document and should be defined at a higher level (Android or Server).	b	Variable
1F8129	Data Format for Data Encryption Proprietary data item that specifies which data format to use for encryption of card data Possible Values: 00h: Poynt Format (Default) (Full Track Data Encrypted, Left-padded with 0's if track format is ASCII and Left-padded with F's if track format is BCD/hex) 02h: Poynt Format (Full Track Data Encrypted, Right-padded with 0's if track format is ASCII and Right-padded with F's if track format is BCD/hex) 03h: Poynt Format (Full Track Data Encrypted, Right-padded with F's if needed) 04h: Poynt Format (Full Track Data Encrypted, Left-padded with F's if needed) 05h: Elavon Format (Full Track Data Encrypted, Right-padded with F's if needed, Track Separator is '=' instead of 'D') 08h: Reserved 09h: Walmart Format (Combined Track Data Encrypted, OAEP padding, no right-padding) Note: This parameter is a Reader parameter and should be set to the same value in each terminal configuration (CT, CL, MSR). If this tag is missing from the terminal configuration for a particular interface, then the Reader may get the value from the terminal configuration of one of the other two interfaces.	b	1
1F8133	Track Data Format 2 This byte can be used in conjunction with Track Data Format (DFDB) to configure the track data. The format of this byte is as follows. Bit 2-7: RFU (must always be set to 0) Bit 1: Use Hex Format for Track Data Bit 0: Use ASCII Format for Track Data	b	1
1F8154	Terminal Configuration Checksum This is the checksum calculated over the critical EMV Terminal Configuration parameters. This field should never be set via *Set Terminal Configuration* command. It is generated on-the-fly from the parameters in the config and is returned via the *Get Terminal Configuration* command. For more details on the checksum, refer to *the Get Firmware Component Version* command.	b	4

Tag	Data Item & Description	Format	Length (in Bytes)
1F8159	ADA-Compliant Keypad Proprietary data item that can be used to configure ADA-Compliant Keypad functionality. Presence: Optional Possible Values: 00h: Disable ADA Support (Default) 01h: Enable ADA Support (“Lock on First Digit” Mode) 02h: Enable ADA Support (“Lock on Toggle Button” Mode) 03h: Enable ADA Support (“Mixed” Mode) Note: If this Tag is missing from the applicable Perform Transaction command, Get Manual Card Data command, Get New DUKPT PIN command and Get New M/S PIN command AND the Terminal Configurations, then the ADA Compliant Keypad functionality will remain disabled by default. Note: If one of the ADA Modes needs to be supported via configuration, then it *must* be set in each Terminal Configuration separately. If we do not set it for the Terminal Configuration for a specific interface but set it for another interface, then the Reader will not try to pick the configuration from one of the other configurations. It will only check the Terminal Configuration for the interface on which the card was detected. Note: When setting the Terminal Configurations, it is important to set the Terminal Configuration for each Interface separately (i.e. not send a single command to set Terminal Configurations for all three interfaces by using Interface = 07h).	b	1
1F8163	CT Interac Config This data item allows configuration of features related to Contact Interac. The format of this data item is as follows: Byte 1: General Configuration The format of this byte is as follows. Bit 7-1: RFU (must always be set to 0) Bit 0: Enable CT Interac-specific Application Selection. This feature MUST be enabled if a Terminal is for the Canadian Market.	b	1
1F820A	PCI Key Management Scheme for Data MAC (For Interac MAC, Safe-T) Possible Values: 00h: Use DUKPT 01h: Use Master/Session (Default) 02h: Not Used	b	1
1F8234	Enable/Disable Enhanced Firmware Logging Possible Values: 00h: Disable Enhanced Firmware Logging (Default) 01h: Enable Enhanced Firmware Logging Presence: Optional Note: If Enhanced Firmware Logging is disabled, then data will not be logged into the enhanced log buffer.	b	1
CFFFFF50	TLV Data Record Tags (Decline / Failure) Proprietary TLV data item that may contain a list of Tags that the Reader should return with the Perform Transaction Response if the Status Code being returned is an Offline or Online Decline or Failed. Presence: Optional.	b	Variable

2.3 Terminal Configuration Data Items for the Contactless Interface

Tag	Data Item & Description	Format	Length (in Bytes)
5F2A	Transaction Currency Code For CL this is a Terminal parameter for all Kernels, but some implementations of the MC and Amex Kernels define it as an AID parameter.	n3	2
5F36	Transaction Currency Exponent	n1	1
5F57	Account Type	n2	1
9C	Transaction Type	n2	1
9F1A	Terminal Country Code	n3	2
9F1E	Interface Device (IFD) Serial Number	8	an 8
9F33	Terminal Capabilities	b	3
9F35	Terminal Type	n2	1
9F40	Additional Terminal Capabilities	b	5
1F8114	PIN Bypass Supported Possible Values: 00h: PIN Bypass not supported. 01h: PIN Bypass supported Whether PIN Bypass is supported or not, how the PIN Entry UI (Enter Button, Cancel Button, Timeout) behave is defined by *PIN Entry UI Config* (Tag 1F8171). Note: This parameter is a Reader parameter and should be set to the same value in each terminal configuration (CT, CL, MSR). If this tag is missing from the terminal configuration for a particular interface, then the Reader may get the value from the terminal configuration of one of the other two interfaces.	b	1
1F8171	PIN Entry UI Config Indicates how the PIN Entry UI should behave. Possible Values: 01h: Behavior 1 - PIN Bypass on Cancel Button (Default) 02h: Behavior 2 - PIN Bypass on Enter Button (If No PIN Entered) For more detailed information on PIN Entry UI Behavior see *Appendix A.4 PIN Entry UI Configuration Behaviors*. Note: This parameter is a Reader parameter and should be set to the same value in each terminal configuration (CT, CL, MSR). If this tag is missing from the terminal configuration for a particular interface, then the Reader may get the value from the terminal configuration of one of the other two interfaces.	b	1
1F8220	Terminal Behavior on Missing PIN Key Indicates how the Terminal should behave if the PIN Encryption Key is missing. Applies to Online PIN encryption key only. Possible Values: 01h: Terminate Transaction on Missing PIN Key (Default) 02h: Continue Transaction on Missing PIN Key and treat This situation as “PIN Entry Required and PIN Pad Not Present or PIN Pad Not Working”	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
1F8226	Terminal Behavior on PIN Entry Timeout Indicates how the Terminal should behave if there was a PIN Entry Timeout (overall or inter-digit timeout). Applies to both Online and Offline PIN entry. Possible Values: 00h: Treat it as “PIN Pad not working” and continue the Transaction (Default) 01h: Treat it as an attempted PIN Bypass. Terminal behavior will depend on whether PIN Bypass is supported or not. Presence: Optional	b	1
1F8230	Enable/Disable RNIB related features for ADA PIN entry. Possible Values 00h: RNIB features disabled 01h: RNIB features enabled RNIB specific features include - Firmware will send *ADA Swiped* notifications during ADA PIN entry after ADA button has been swiped. - Firmware will NOT beep after ADA PIN digit entry double tap. The beep will be handled by Android - Inter-digit time out would be 3 minutes instead of 1 minute - ADA digit input requires double tap after swipe instead of single tap - ADA input swipe criteria reduced i.e. shorter ADA swipes accepted as valid.	b	1
1F8227	Outcome Parameter Set Format Possible Values: 05h: Outcome Parameter Set in JCB Format 07h: Outcome Parameter Set in CUP Format Presence: Optional (Only required for CL JCB and CL CUP Certification)	b	1
1F8228	Use JCB Parsing Allows enabling of JCB-specific TLV parsing thus overriding normal TLV parsing in some error situations. By default, normal BER TLV parsing is used as per EMV requirements. Possible Values: 01h: Use JCB-specific TLV parsing Other: Use Normal TLV parsing Presence: Optional. Normally this parameter should not be used. Note: JCB-specific TLV parsing should normally not be used since it overrides normal EMV-specified BER TLV parsing in the Application Selection phase in order to recover from some error conditions which is not mandated or allowed in normal EMV. It should ONLY be used for certification testing and in environments where this functionality is specifically required.	b	1
DF812D	Message Hold Time	b	3
DFDB	MSD Track Data Format Specifies Track 1 and Track 2 data format for non EMV transactions. Possible values: 00h: SS, ES and LRC are not included in the track data. 01h: SS & ES are included in the track data but LRC is not. 02h: SS, ES and LRC are included in the track data.	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
DFDD	Debug Logging Enabled. Possible values: 00h: Log all errors, warnings, information & debug 01h: Log all errors, warnings & information 02h: Log all errors, warnings & important information 03h: Log all errors & warnings 04h: Log all errors 05h: Log critical errors FFh: Disable all logging (default value if this tag is absent)	b	1
DFDF	Exception List Processing Supported	b	1
DFFFDF00	Contactless not Allowed Enabled (Visa) If during pre-processing all applications have this indicator set to false, the kernel will still allow the transaction to start if tag equals zero. Default Value should be set to enabled i.e. 01h.	b	1
1F8130	Terminal Supported Languages The list of languages supported by the Terminal. Each language in this list is represented by 2 alphabetical characters as defined in ISO 639. For example, in the following TLV definition 1F81300C656E707466727A6872756573 The parsed data is as follows: 656E = “en” = English 7074 = “pt” = Portuguese 6672 = “fr” = French 7A68 = “zh” = Chinese 7275 = “ru” = Russian 6573 = es = Spanish Note: From the terminal side the language code must always be in lower case letters, however, the Reader should accept both lower and upper case codes. See Appendices for Overview of Multi-Language Support.	an2	Variable
1F8131	Configuration Version Version of the terminal configuration for the contactless interface. This is an optional field and can be used to store a version or a configuration identifier. The actual contents or format of this field are out of the scope of this document and should be defined at a higher level (Android or Server).	b	Variable

Tag	Data Item & Description	Format	Length (in Bytes)
1F8129	Data Format for Data Encryption Proprietary data item that specifies which data format to use for encryption of card data Possible Values: 00h: Poynt Format (Default) (Full Track Data Encrypted, Left-padded with 0's if track format is ASCII and Left-padded with F's if track format is BCD/hex) 02h: Poynt Format (Full Track Data Encrypted, Right-padded with 0's if track format is ASCII and Right-padded with F's if track format is BCD/hex) 03h: Poynt Format (Full Track Data Encrypted, Right-padded with F's if needed) 04h: Poynt Format (Full Track Data Encrypted, Left-padded with F's if needed) 05h: Elavon Format (Full Track Data Encrypted, Right-padded with F's if needed, Track Separator is '=' instead of 'D') 08h: Reserved 09h: Walmart Format (Combined Track Data Encrypted, OAEP padding, no right-padding) Note: This parameter is a Reader parameter and should be set to the same value in each terminal configuration (CT, CL, MSR). If this tag is missing from the terminal configuration for a particular interface, then the Reader may get the value from the terminal configuration of one of the other two interfaces.	b	1
1F8133	Track Data Format 2 This byte can be used in conjunction with Track Data Format (DFDB) to configure the track data. The format of this byte is as follows. Bit 2-7: RFU (must always be set to 0) Bit 1: Use Hex Format for Track Data Bit 0: Use ASCII Format for Track Data	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
1F8159	ADA-Compliant Keypad Proprietary data item that can be used to configure ADA-Compliant Keypad functionality. Presence: Optional Possible Values: 00h: Disable ADA Support (Default) 01h: Enable ADA Support (“Lock on First Digit” Mode) 02h: Enable ADA Support (“Lock on Toggle Button” Mode) 03h: Enable ADA Support (“Mixed” Mode) Note: If this Tag is missing from the applicable Perform Transaction command, Get Manual Card Data command, Get New DUKPT PIN command and Get New M/S PIN command AND the Terminal Configurations, then the ADA Compliant Keypad functionality will remain disabled by default. Note: If one of the ADA Modes needs to be supported via configuration, then it *must* be set in each Terminal Configuration separately. If we do not set it for the Terminal Configuration for a specific interface but set it for another interface, then the Reader will not try to pick the configuration from one of the other configurations. It will only check the Terminal Configuration for the interface on which the card was detected. Note: When setting the Terminal Configurations, it is important to set the Terminal Configuration for each Interface separately (i.e. not send a single command to set Terminal Configurations for all three interfaces by using Interface = 07h).	b	1
1F817B	Switch from CL to CT Interface on Card Insert Some contactless schemes have a requirement to switch from CL to CT Interface if a Card is inserted into the Reader during a contactless transaction. This tag can be used to configure whether this functionality is to be enabled before we know that the contactless card belongs to such a scheme. The format of this data item is as follows: Bit 7-1: RFU (must always be set to 0) Bit 0: Allow CL to CT Interface switching during Entry Point. Presence: Optional. Applies to: CL Visa, CL CUP International	b	1
1F820A	PCI Key Management Scheme for Data MAC (For Interac MAC, Safe-T) Possible Values: 00h: Use DUKPT 01h: Use Master/Session (Default) 02h: Not Used	b	1
1F8234	Enable/Disable Enhanced Firmware Logging Possible Values: 00h: Disable Enhanced Firmware Logging (Default) 01h: Enable Enhanced Firmware Logging Presence: Optional Note: If Enhanced Firmware Logging is disabled, then data will not be logged into the enhanced log buffer.	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
CFFFFF50	TLV Data Record Tags (Decline / Failure) Proprietary TLV data item that may contain a list of Tags that the Reader should return with the Perform Transaction Response if the Status Code being returned is an Offline or Online Decline or Failed. Presence: Optional.	b	Variable

2.4 Terminal Configuration Data Items for the MSR Interface

Tag	Data Item & Description	Format	Length (in Bytes)
5F57	Account Type	n2	1
DFDB	Track Data Format Specifies Track 1 and Track 2 data format for MSR transactions. Possible values: 00h: SS, ES and LRC are not included in the track data. 01h: SS & ES are included in the track data but LRC is not. 02h: SS, ES and LRC are included in the track data.	b	1
1F8114	PIN Bypass Supported Possible Values: 00h: PIN Bypass not supported. 01h: PIN Bypass supported Whether PIN Bypass is supported or not, how the PIN Entry UI (Enter Button, Cancel Button, Timeout) behave is defined by *PIN Entry UI Config* (Tag 1F8171). Note: This parameter is a Reader parameter and should be set to the same value in each terminal configuration (CT, CL, MSR). If this tag is missing from the terminal configuration for a particular interface, then the Reader may get the value from the terminal configuration of one of the other two interfaces.	b	1
1F8171	PIN Entry UI Config Indicates how the PIN Entry UI should behave. Possible Values: 01h: Behavior 1 - PIN Bypass on Cancel Button (Default) 02h: Behavior 2 - PIN Bypass on Enter Button (If No PIN Entered) For more detailed information on PIN Entry UI Behavior see *Appendix A.4 PIN Entry UI Configuration Behaviors*. Note: This parameter is a Reader parameter and should be set to the same value in each terminal configuration (CT, CL, MSR). If this tag is missing from the terminal configuration for a particular interface, then the Reader may get the value from the terminal configuration of one of the other two interfaces.	b	1
1F8220	Terminal Behavior on Missing PIN Key Indicates how the Terminal should behave if the PIN Encryption Key is missing. Applies to Online PIN encryption key only. Possible Values: 01h: Terminate Transaction on Missing PIN Key (Default) 02h: Continue Transaction on Missing PIN Key and treat This situation as “PIN Entry Required and PIN Pad Not Present or PIN Pad Not Working”	b	1
1F8226	Terminal Behavior on PIN Entry Timeout Indicates how the Terminal should behave if there was a PIN Entry Timeout (overall or inter-digit timeout). Applies to both Online and Offline PIN entry. Possible Values: 00h: Treat it as “PIN Pad not working” and continue the Transaction (Default) 01h: Treat it as an attempted PIN Bypass. Terminal behavior will depend on whether PIN Bypass is supported or not. Presence: Optional	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
1F8230	Enable/Disable RNIB related features for ADA PIN entry. Possible Values 00h: RNIB features disabled 01h: RNIB features enabled RNIB specific features include - Firmware will send *ADA Swiped* notifications during ADA PIN entry after ADA button has been swiped. - Firmware will NOT beep after ADA PIN digit entry double tap. The beep will be handled by Android - Inter-digit time out would be 3 minutes instead of 1 minute - ADA digit input requires double tap after swipe instead of single tap - ADA input swipe criteria's reduced	b	1
1F812F	Custom BIN Range List This list specifies one or more records, with each record specifying a BIN range. MSR cards whose BINs match any of the BINs in the ranges specified in this list will be treated as payment cards and the sensitive card data will be encrypted, as is done for payment MSR cards. Note: This configuration parameter is to be used only to define non-payment cards as payment cards so that they can be encrypted. For PCI Compliance, the list of all known Payment Card BIN ranges is hard-coded in the firmware and those hard-coded BIN Ranges cannot be changed or disabled dynamically via this parameter. The format of each record will be as given below Byte 1: Number of numeric digits in each BIN. This can have a value from 01h to 06h. Bytes 2-4: Lower BIN Limit This represents the lower limit of the BIN range (i.e. the lower limit of the initial PAN digits). This is a 3-byte field that contains the BIN (initial PAN digits) encoded as BCD i.e. each numeric digit is encoded in one nibble and if the number of numeric digits is less than 6, then it is left-padded with zeros. For example, the 6-digit BIN 308512 will be represented as 0x30, 0x85, 0x12 And the 3-digit BIN 123 will be represented as 0x00, 0x01,0x23 Bytes 5-7: Upper BIN Limit This represents the upper limit of the BIN range (i.e. the lower limit of the initial PAN digits). The format will be similar to the format of the Lower BIN Limit. Examples of records are given below. - A BIN Range of 308512 to 308514 will be represented as 0x06, 0x30, 0x85, 0x12, 0x30, 0x85, 0x14 - A BIN Range of 650 to 659 will be represented as 0x03, 0x00, 0x06, 0x50, 0x00, 0x06, 0x59	b	Variable (Max 128)

Tag	Data Item & Description	Format	Length (in Bytes)
1F8131	Configuration Version Version of the terminal configuration for the MSR interface. This is an optional field and can be used to store a version or a configuration identifier. The actual contents or format of this field are out of the scope of this document and should be defined at a higher level (Android or Server).	b	Variable
1F8127	PCI Key Management Scheme for PIN Encryption Proprietary data item that specifies the key management scheme to use for PIN encryption. Possible Values: 00h: Use DUKPT (Default) 01h: Use Master/Session Note: This parameter is a Reader parameter and should be set to the same value in each terminal configuration (CT, CL, MSR). If this tag is missing from the terminal configuration for a particular interface, then the Reader may get the value from the terminal configuration of one of the other two interfaces.	b	1
1F8128	PCI Key Management Scheme for Data Encryption Proprietary data item that specifies the key management scheme to use for data encryption. The key management scheme specified here will be used for data encryption regardless of what data format has been configured (see next data item). Possible Values: 00h: Use DUKPT (Default) 01h: Use Master/Session 02h: Use RSA Note: Currently this value is used only by the *Get Manual Card Data* command. Note: This parameter is a Reader parameter and should be set to the same value in each terminal configuration (CT, CL, MSR). If this tag is missing from the terminal configuration for a particular interface, then the Reader may get the value from the terminal configuration of one of the other two interfaces.	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
1F8129	Data Format for Data Encryption Proprietary data item that specifies which data format to use for encryption of card data Possible Values: 00h: Poynt Format (Default) (Full Track Data Encrypted, Left-padded with 0's if track format is ASCII and Left-padded with F's if track format is BCD/hex) 02h: Poynt Format (Full Track Data Encrypted, ~~Right-padded with zeros if needed)~~ Right-padded with 0's if track format is ASCII and Right-padded with F's if track format is BCD/hex) 03h: Poynt Format (Full Track Data Encrypted, Right-padded with F's if needed) 04h: Poynt Format (Full Track Data Encrypted, Left-padded with F's if needed) 05h: Elavon Format (Full Track Data Encrypted, Right-padded with F's if needed, Track Separator is '=' instead of 'D') 08h: Reserved 09h: Walmart Format (Combined Track Data Encrypted, OAEP padding, no right-padding) Note: This parameter is a Reader parameter and should be set to the same value in each terminal configuration (CT, CL, MSR). If this tag is missing from the terminal configuration for a particular interface, then the Reader may get the value from the terminal configuration of one of the other two interfaces.	b	1
1F8133	Track Data Format 2 This byte can be used in conjunction with Track Data Format (DFDB) to configure the track data. The format of this byte is as follows. Bit 2-7: RFU (must always be set to 0) Bit 1: Use Hex Format for Track Data Bit 0: Use ASCII Format for Track Data	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
1F8132	Auto-Detect MSR Debit Normally the Reader determines whether the MSR Transaction is to be treated as a Debit Card (Online PIN required) based on the Account Type if this field is present in the command data. The Auto-Detect MSR Debit configuration parameter can be used to tell the Reader to decide whether to treat the MSR Card as a Debit Card based on the Service Code in the track data. If there is no Service Code, then it will default to using the Account Type (if available). Possible Values: 00h: Do not perform auto-detection of debit card based on Service Code. Only the Account Type will be used in this case. (Default Behavior) If Account Type is Cheque/Debit, PIN will be required. For any other value of Account Type, PIN will not be required. For MSR Bancomat Track3 PIN will be required. 01h: Perform auto-detection of debit-card based on Service Code. If there is no Service Code, then the Account Type Will be used in this case. For MSR Bancomat Track3 PIN will be required. FEh: Same as FFh, except that for MSR Bancomat Track 3 PIN will be required. FFh: Do not perform auto-detection of debit card i.e. bypass auto-detection using both the Account Type as well as the Service Code. In this case auto-detection of Debit Card is not performed by the Reader but may be performed by the Merchant Terminal. If a PIN is required, then the Terminal may request it using the *Get Manual Card Data* command.	b	1
1F8159	ADA-Compliant Keypad Proprietary data item that can be used to configure ADA-Compliant Keypad functionality. Presence: Optional Possible Values: 00h: Disable ADA Support (Default) 01h: Enable ADA Support (“Lock on First Digit” Mode) 02h: Enable ADA Support (“Lock on Toggle Button” Mode) 03h: Enable ADA Support (“Mixed” Mode) Note: If this Tag is missing from the applicable Perform Transaction command, Get Manual Card Data command, Get New DUKPT PIN command and Get New M/S PIN command AND the Terminal Configurations, then the ADA Compliant Keypad functionality will remain disabled by default. Note: If one of the ADA Modes needs to be supported via configuration, then it *must* be set in each Terminal Configuration separately. If we do not set it for the Terminal Configuration for a specific interface but set it for another interface, then the Reader will not try to pick the configuration from one of the other configurations. It will only check the Terminal Configuration for the interface on which the card was detected. Note: When setting the Terminal Configurations, it is important to set the Terminal Configuration for each Interface separately (i.e. not send a single command to set Terminal Configurations for all three interfaces by using Interface = 07h).	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
1F8170	MSR Track Standards Config Indicates which Track Standards are supported in addition to ISO 7813 for MSR-Only cards when decoding track data. Applies to MSR Transactions Only Presence: Optional Format: Bit 0: ANSI X4.16 Supported (Default = 0) Bit 1: Treat Track3 as Bancomat Track3 (Default=0) (*Reserved for Future Use*) Bit 2-7: RFU (must always be set to 0)	b	1
1F822C	MSR Flags This parameter contains flags to control MSR Transaction and behavior. Applies to MSR Transactions Only Presence: Optional The format of this byte is as follows. Bit 1-7: RFU (must always be set to 0) Bit 0: Prompt for MSR Card Removal (Default = 0) After transaction completed. This is done by sending the "Card Not Removed" UI Notification.	b	1
1F8234	Enable/Disable Enhanced Firmware Logging Possible Values: 00h: Disable Enhanced Firmware Logging (Default) 01h: Enable Enhanced Firmware Logging Presence: Optional Note: If Enhanced Firmware Logging is disabled, then data will not be logged into the enhanced log buffer.	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
3F8106	Acquirer Data for Non-Bancomat MSR Tracks (*Reserved for Future Use*) This is a single constructed tag that may contain one or more instances of *MSR Single Acquirer Data* (Tag 3F8107) data items. There will be one instance of 3F8107 per acquirer. Each MSR Single Acquirer Data (Tag 3F8107) is, in turn, a constructed tag that may contain various data items related to the associated acquirer such as • Acquirer Identifier • Acquirer Name • PIN-Block Protection Key Index (KIP Index) • Financial Message Protection Key Index (KPOS Index) • BIN Range List for Acquirer See the Table *Data Items in MSR Single Acquirer Data* for more details on these data items. The tag hierarchy is given below. <Acquirer Data for Non-Bancomat MSR Tracks (3F8106)> <MSR Single Acquirer Data (3F8107)> <Acquirer Identifier> <Acquirer Name> <PIN-Block Protection Key Index (KIP Index)> <Financial Msg Protection Key Index (KPOS Index)> <BIN Range List for Acquirer> <MSR Single Acquirer Data (3F8107)> <…> <…> <MSR Single Acquirer Data (3F8107)> <…>	b	Variable
3F8108	Acquirer Data for Bancomat MSR Track (*Reserved for Future Use*) This is a single constructed data item containing information about the Acquirer for Bancomat MSR Track. This data item may contain tags related to the acquirer for Bancomat MSR such as • Acquirer Identifier • Acquirer Name • AP Protection Key Index (KAP Index) • Financial Message Protection Key Index (KPOS Index) See the Table *Data Items in Acquirer Data for Bancomat MSR Track* for more details on these data items. The tag hierarchy is given below. <Acquirer Data for Bancomat MSR Tracks (3F8108)> <Acquirer Identifier> <Acquirer Name> <AP Protection Key Index (KAP Index)> <Financial Msg Protection Key Index (KPOS Index)>	b	Variable

3 AID Configuration

The Poynt Configuration Service maintains a separate configuration for each AID supported by the terminal. Further, the configuration for a contactless AID will be maintained separately from the configuration for a

contact AID. The AID configurations are retained over power cycles.

When the Card Reader powers up for the first time, it is assumed to have no AID configurations. In this case the Reader should itself set some default AID configurations for contactless as well as for the contact interface based on the defaults defined in it's corresponding firmware. Once the initial default AID configurations are set for each card interface, the Reader should not automatically set or change the AID configuration at the next power up or at any other time unless new configuration has been loaded through Poynt Configuration service.

The AID configuration applies only to the specific AID and Card Interface. When the Reader receives this configuration, it should use the "mode" to determine whether the config should be modified or overwritten. Possible values of the Mode field are
00: Modify
01: Overwrite

If the Mode is set to "Modify", the Reader should not delete the existing AID configuration for the specified interface but will perform a non-destructive modification of the AID configuration. If a tag already exists in the existing AID configuration, the Reader should just modify the length and value. If a tag is not present in the existing AID configuration, the Reader should append the new TLV.

If the Mode is set to "Overwrite" then it should delete the entire existing AID configuration for the specified card interface and overwrite it with the configuration TLVs specified in the command data. Before deleting the existing configuration, it should make sure that the command data does not contain any mall formatted TLVs and that all mandatory TLVs are present.

If a TLV included in an AID configuration is also defined for the Terminal configuration for the relevant card interface, then the value of the TLV defined in the AID configuration will override the value in the Terminal configuration when it is loaded.

Further any TLVs included in an AID configuration that are not defined here will not be rejected by the Reader and will be saved in the AID configuration.

3.1 AID Configuration Data Format Common to all Card Interfaces

Tag	Data Item & Description	Format	Length (in Bytes)
- mode	Mode The Mode field indicates whether to modify the configuration or to perform a destructive overwrite. Possible values are 00: Modify 01: Overwrite Presence: Mandatory.	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
- cardInterface	Card Interface Indicates the card interface for which to set this AID configuration. The format of this byte is given below. Bit 0: Reserved bit (must always be set to 0) Bit 1: Contactless AID. Bit 2: Contact AID. Bits 3-7: RFU. The RFU bits must be set to 0. Only one of the defined bits can be set at a time. Therefore this field can have one of two values: 02h = Contactless AID 04h = Contact AID Presence: Mandatory.	b	1
aid	Application Identifier (AID) – Terminal Presence: Mandatory	b	5-16
data	The above AID configuration TLVs may be followed by other AID configuration TLVs that are card scheme specific. These TLV Tags are given in the tables below.		

3.2 AID Configuration Data Format specific to Contact EMV AIDs

Tag	Data Item & Description	Format	Length (in Bytes)
1F8113*	Application Selection Indicator. Indicates whether the terminal should match the AID and AID Length in the card exactly or only up to the length of the AID in the terminal. Possible Values: 00 = Partial Selection Not Allowed. Must match full AID and length. 01 = Partial Selection Allowed. Presence: Mandatory	b	1
1F8131	Configuration Version Version of the AID configuration for a contact EMV AID. This is an optional field and can be used to store a version or a configuration identifier. The actual contents or format of this field are out of the scope of this document and should be defined at a higher level (Android or Server).	b	Variable
97	Default TDOL This value of TDOL is used if the card does not provide a TDOL. As per EMV, this is a per AID data. Note: As per EMV Spec 97 is the tag for TDOL (Card-resident) but we are using it for Terminal-resident Default TDOL as well. The Kernel will first look for TDOL in the Card Tag List and if it does not find it there it will look in the Terminal Tag List.	b	Variable
9F01	Acquirer Identifier	n6-11	3-6
9F09	Application Version Number (Terminal)	b	2
9F15	Merchant Category Code	n 4	2
9F16	Merchant Identifier	ans 15	15
9F1B	Terminal Floor Limit	b	4
9F1C	Terminal ID	an 8	8
9F1D	Terminal Risk Management Data Application-specific value used by the card for risk management.	b	1-8
9F3C	Transaction Reference Currency Code	n 3	2
9F3D	Transaction Reference Currency Exponent	n1	1
9F4E	Merchant Name and Location	ans	Variable
CFFFFF00	Data Record Tags (EMV)	b	Variable
DF31	Financial Message Protection key index (*Reserved for Future Use*)	b	3
DF34	PIN Block Protection key index (*Reserved for Future Use*)	b	3
DF35	AP Protection key index (*Reserved for Future Use*)	b	3
DF38	Acquirer Name (*Reserved for Future Use*)	ans	Variable
E001 ~~DF8120~~	Terminal Action Code – Default For Contact EMV, Credit Call defines this as Tag ~~9F0D or~~ E001.	b	5
E002 ~~DF8121~~	Terminal Action Code – Denial For Contact EMV, Credit Call defines this as Tag ~~9F0E or~~ E002.	b	5
E003 ~~DF8122~~	Terminal Action Code – Online For Contact EMV, Credit Call defines this as Tag ~~9F0F or~~ E003.	b	5

Tag	Data Item & Description	Format	Length (in Bytes)
9F49	Default DDOL This value of DDOL is used if the card does not provide a DDOL. As per EMV, this is a per AID data. Note: As per EMV Spec 9F49 is the tag for DDOL (Card-resident) but we are using it for Terminal-resident Default DDOL as well. The Kernel will first look for DDOL in the Card Tag List and if it does not find it there it will look in the Terminal Tag List.	b	Variable
E015	Threshold Value for Biased Random Selection Applies to: CT, CL	b	4
E013	Target Percentage to be used for Random Selection Applies to: CT, CL	b	4
E014	Maximum Target Percentage to be used for Biased Random Selection Applies to: CT, CL	b	4
1F8122	CT to MSR Fallback Configuration This data item allows configuration of Contact (Chip) to MSR fallback based on EMV, various card association, acquirer or regional (L3) rules. The format of this data item is as follows: Byte 1: Disable “Contact (Chip) Card to MSR Fallback” By default, “Contact to MSR fallback” is supported. However, this data item can be used to disable support for this feature. Possible Values 00h: Contact Card to MSR Fallback supported. This is the default if this data item is not present. 01h: Disable “Contact Card to MSR Fallback” support. If CT to MSR fallback is supported, then the standard method for fallback specified by EMV will always be supported. However, support for non-standard fallback methods can be configured via Byte 2. Byte 2: Non-EMV Fallback Methods Supported. This byte can be used to configure only the non-standard fallback methods that are usually outside the scope of EMV and are usually specified by the card associations, acquirers or regional rules. The format of this byte is as follows. Bit 7: Enable Fallback on Empty Candidate List Bit 6: Enable Fallback on Card Blocked Bit 5: Enable Fallback on App Blocked Bit 4: Enable Fallback on Chip Read Error during App Sel Bit 3: Enable Fallback on Chip Read Error during GPO Bit 2: Enable Fallback on Chip Read Error during Read Recs Bit 1: Enable Fallback on Chip Read Error during Gen AC 1 Bit 0: Enable Fallback on Chip Read Error During Gen AC 2 Byte 3: RFU (must always be set to 00h)	b	3
1F816F	Enforce MAC The format of this data item is as follows: Byte 1: Bit 7-2: RFU (must always be set to 0) Bit 1: Interac Safe-T Enabled Bit 0: Enforce Interac MACing on this AID Applies to CT Interac AIDs only.	b	Variable (Max 4)

Tag	Data Item & Description	Format	Length (in Bytes)
1F822B	Multiple Application Version Numbers (Terminal) Applies to: CT Only Presence: Optional This field contains one or more Application Version Number (Terminal) values supported for the specified AID. Each AVN (Terminal) value occupies two bytes. Therefore, up to 10 AVN (Terminal) values (20 bytes) can be stored in this parameter. During a transaction, after READ RECORDS, if the card returns the AVN (ICC) (Tag 9F08) and if the 1F822B tag is present for the selected AID, then the Reader compares the value of AVN (ICC) (Tag 9F08) with each of the AVN (Terminal) values in the 1F822B parameter. If the AVN (ICC) matches any of the values in the 1F822B tag, then the Reader sets the value of AVN (Terminal) i.e. Tag 9F09 in the CT EMV L2 Kernel database to the matching value and then continues the transaction as normal.	b	Variable (Max 20)

3.3 Data Items specific to Contactless Visa AIDs (Kernels 1 & 3)

Tag	Data Item & Description	Format	Length (in Bytes)
1F8119	AID Enabled Default: Enabled (if Tag is absent)	b	1
DF810C	Kernel ID Valid Value: 03h for CL Visa Kernel (VCPS)	b	1
1F8131	Configuration Version Version of the AID configuration for a contactless Visa AID. This is an optional field and can be used to store a version or a configuration identifier. The actual contents or format of this field are out of the scope of this document and should be defined at a higher level (Android or Server).	b	Variable
3F8005	Dynamic Reader Limits Set (DRL Set) Multiple instances of DRL Set may be defined in an AID configuration. A DRL Set comprises of a number of data items encapsulated within the DRL Set tag. A list of these nested data items is given in the next table.	B	Variable
9F1B	Terminal Floor Limit	b	4
9F4E	Merchant Name and Location	ans	Variable
9F66	Terminal Transaction Qualifiers (TTQ) This field is formatted as follows: Byte 1: Bit 7: MSD supported Bit 6: RFU (must always be set to 0) Bit 5: qVSDC supported Bit 4: EMV contact chip supported Bit 3: Offline-only reader Bit 2: Online PIN supported Bit 1: Signature supported Bit 0: Offline Data Authentication for Online Authorizations supported Byte 2: Bit 7: Online cryptogram required Bit 6: CVM required Bit 5: (Contact Chip) Offline PIN supported Bit 4-0: RFU (00000b) Byte 3: Bit 7: Issuer Update Processing supported Bit 6: Mobile functionality supported (Consumer Device CVM) Bit 5-0: RFU (000000b) Byte 4: RFU (00h)	b	4
9F7A	VLP Terminal Support Indicator 00 = Online only solution supported 01 = Offline/Online solution supported		
CFFF8001	Visa MSD CVN17 Supported (in Magstripe Mode) 00h: Visa MSD CVN17 is not supported. 01h: Visa MSD CVN17 is supported (default).	b	1
CFFF8002	Visa DRL Enabled 00h: DRL not enabled. 01h: DRL Enabled.	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
CFFFFF00	Data Record Tags (EMV)	b	Variable
CFFFFF01	Data Record Tags (MSD / Magstripe / Non-EMV)	b	Variable
CFFFFF02	Select by AID Supported (Select via List of AIDs Supported?) Possible Values: 00h: Select by AID is not supported (Default). 01h: Select by AID is supported. 02h: Select by AID should only be performed if the condition is met (Amex XP 3.0). 03h: Select by AID should only be performed if the condition is met (Amex XP 3.1). For stops and comms failure Select by AID should not be performed.	b	1
CFFFFF03	Discretionary Data Tags (EMV)	b	Variable
CFFFFF04	Discretionary Data Tags (MSD / Magstripe / Non-EMV)	b	Variable
CFFFFF05	Optional Data Record Tags (MSD / Magstripe / Non-EMV)	b	Variable
CFFFFF50	Data Record Tags (Decline / Failure)	b	Variable
DFDE	Zero Amount Mode Possible values: 00h: EMV-compliant mode supported. 01h: Kernel should not force zero amount transactions online. 02h: Transaction currency should be set to the card currency. 04h: A 1p/1c amount should be used instead of zero These values may be combined to indicate multiple features.	b	1
DFE1	Status Check Supported	b	1
DFE2	Terminal Contactless Transaction Limit	b	4
DFE3	Terminal Contactless Floor Limit	b	4
DFE4	Terminal CVM Required Limit	b	4
DFE5	Zero Amount Allowed 00h: Zero amount transactions are not supported. 01h: Zero amount transactions are supported.	b	1
DFFFDF00	Contactless not Allowed Enabled Indicates that for Visa certification, if during pre-processing all applications have this indicator set to false, the kernel will still allow the transaction to start if tag equals zero. Default Value should be set to enabled i.e. 01h.	b	1
DFFFDF01	Visa AP Kernel Supported	b	1
DFFFDF02	Reader Contactless Transaction Limit	n 12	6
DFFFDF03	Reader Contactless Floor Limit	n 12	6
DFFFDF04	Reader CVM Required Limit	n 12	6

The data items contained in a DRL Set are given in the following table.

Tag	Data Item & Description	Format	Length (in Bytes)
9F5A	Application Program ID	b	1-16

Tag	Data Item & Description	Format	Length (in Bytes)
DFFFDF41	DRL Status Check Supported 00h: Status Check is not supported 01h: Status Check is supported.	b	1
DFFFDF42	DRL Terminal Contactless Transaction Limit	b	4
DFFFDF43	DRL Terminal Contactless Floor Limit	b	4
DFFFDF44	DRL Terminal CVM Required Limit	b	4
DFFFDF45	DRL Zero Amount Allowed 00h: Zero Amount transactions are not supported (Option 2). 01h: Zero Amount transactions are supported and online cryptogram required (Option 1)	b	1
DFFFDF46	DRL Risk Checks Enabled The format and meaning of this data item is given below: Bit 0: Status Check Enabled. Bit 1: Transaction Limit Amount Check Enabled. Bit 2: CVM Required Limit Amount Check Enabled. Bit 3: Floor Limit Amount Check Enabled. Bit 4: Zero Amount Check Enabled. Bit 5: Offline-Only Zero Amount Check Enabled. Bit 6,7: RFU (must always be set to 0). Possible Values: 00h: No checks are enabled. 01h: Status Check is enabled. 02h: Transaction Limit Amount Check is enabled. 04h: CVM Required Limit Amount Check is enabled. 08h: Floor Limit Amount Check is enabled. 10h: Zero Amount Check is enabled. 20h: Offline-Only Zero Amount Check is enabled. The above bits/values can be combined to indicate multiple being enabled checks. If this data item is absent then by default all checks will be enabled except Status Check.	b	1
DFFFDF47	DRL Reader Contactless Transaction Limit (Numeric)	n 12	6
DFFFDF48	DRL Reader Contactless Floor Limit (Numeric)	n 12	6
DFFFDF49	DRL Reader CVM Required Limit (Numeric)	n 12	6

3.4 Data Items specific to Contactless MasterCard PayPass AIDs (Kernel 2)

Tag	Data Item & Description	Format	Length (in Bytes)
1F8119	AID Enabled	b	1
DF810C	Kernel ID Valid Value: 02h for CL Mastercard Kernel	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
1F8131	Configuration Version Version of the AID configuration for a contactless Mastercard AID. This is an optional field and can be used to store a version or a configuration identifier. The actual contents or format of this field are out of the scope of this document and should be defined at a higher level (Android or Server).	b	Variable
5F2A	Transaction Currency Code For CL this is a Terminal parameter for all Kernels including MasterCard[1], but the sample configuration for MC Kernel defines it as an AID parameter for some reason.	n3	2
5F57	Account Type	n2	1
9F01	Acquirer Identifier	n 6-11	3-6
9F09	Application Version Number (Terminal)	b	2
9F15	Merchant Category Code	n 4	2
9F16	Merchant Identifier	ans 15	15
9F1A	Terminal Country Code	n3	2
9F1C	Terminal ID	8	an 8
9F1D	Terminal Risk Management Data Application-specific value used by the card for risk management.	b	1-8
9F33	Terminal Capabilities	b	3
9F35	Terminal Type	n2	1
9F40	Additional Terminal Capabilities	b	5
9F4E	Merchant Name and Location	ans	Variable
9F53	Transaction Category Code	an	1
9F5C	DS Requested Operator ID	b	8
9F6D	Application Version Number, Magstripe (Reader)	b	2
9F7C	Merchant Custom Data	b	20
9F7E	Mobile Support Indicator	b	1
CFFFFF00	Data Record Tags (EMV)	b	Variable
CFFFFF01	Data Record Tags (MSD / Magstripe / Non-EMV)	b	Variable
CFFFFF02	Select by AID Supported (Select via List of AIDs Supported?) Possible Values: 00h: Select by AID is not supported (Default). 01h: Select by AID is supported. 02h: Select by AID should only be performed if the condition is met (Amex XP 3.0). 03h: Select by AID should only be performed if the condition is met (Amex XP 3.1). For stops and comms failure Select by AID should not be performed.	b	1
CFFFFF03	Discretionary Data Tags (EMV)	b	Variable
CFFFFF04	Discretionary Data Tags (MSD / Magstripe / Non-EMV)	b	Variable
DF60	DS Input (Card)	b	8
DF62	DS ODS Info	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
DF63	DS ODS Term	b	Variable up to 160
DF8104	Balance Read Before Gen AC	n 12	6
DF8105	Balance Read After Gen AC	n 12	6
DF8108	DS AC Type	b	1
DF8109	DS Input (Term)	b	8
DF810A	DS ODS Info for Reader	b	1
DF810C	Kernel ID Valid Value: 02h for Mastercard Kernel	b	1
DF810D	DSVN Term	b	Variable
DF8110	Proceed to First Write Flag	b	1
DF8112	Tags to Read	b	Variable
DF8117	Card Data Input Capability	b	1
DF8118	CVM Capability – CVM Required	b	1
DF8119	CVM Capability – No CVM Required	b	1
DF811A	Default UDOL	b	3
DF811B	Kernel Configuration	b	1
DF811C	Max Lifetime of Torn Transaction Log Record	b	2
DF811D	Max Number of Torn Transaction Log Records	b	1
DF811E	Magstripe CVM Capability – CVM Required	b	1
DF811F	Security Capability	b	1
DF8120	Terminal Action Code – Default (CL Only) (For CT it is E001)	b	5
DF8121	Terminal Action Code – Denial (CL Only) (For CT it is E002)	b	5
DF8122	Terminal Action Code – Online (CL Only) (For CT it is E002)	b	5
DF8123	Reader Contactless Floor Limit For other Kernels the CC proprietary tag DFFFDF03 is used for this.	n 12	6
DF8124	Reader Contactless Transaction Limit (No On-device CVM)	n 12	6
DF8125	Reader Contactless Transaction Limit (On-device CVM)	n 12	6
DF8126	Reader CVM Required Limit For other Kernels the CC proprietary tag DFFFDF04 is used for this.	n 12	6
DF812C	Magstripe CVM Capability – No CVM Required	b	1
DF812D	Message Hold Time	n6	3
DF8130	Hold Time Value (Field)	b	1
DF8131	Phone Message Table The Tag used for this in CL EMV v2.3 Book C-2 for Kernel 2 is DF8131, however, for some reason the Mastercard Kernel uses DF807F	b	Variable
DF8132	Minimum Relay Resistance Grace Period	b	2
DF8133	Maximum Relay Resistance Grace Period	b	2
DF8134	Terminal Expected Transmission Time for Relay Resistance C-APDU	b	2

Tag	Data Item & Description	Format	Length (in Bytes)
DF8135	Terminal Expected Transmission Time for Relay Resistance R-APDU	b	2
DF8136	Relay Resistance Accuracy Threshold	b	2
DF8137	Relay Resistance Transmission Time Mismatch Threshold	b	1
3F8000	Virtual Dataset Data Items for Transaction Type 00 (Purchase)[2]	b	Variable
3F8001	Virtual Dataset Data Items for Transaction Type 01 (Cash Advance)[2]	b	Variable
3F8002	Virtual Dataset Data Items for Transaction Type 09 (Purchase with Cashback)[2]	b	Variable
3F8003	Virtual Dataset Data Items for Transaction Type 20 (Refund)[2]	b	Variable
3F8006	Virtual Dataset Data Items for Transaction Type 21 (Cash Deposit)[2]	b	Variable
3F8007	Virtual Dataset Data Items for Transaction Type 88 (Invalid - for test purposes only)[2]	b	Variable
3F8008	Virtual Dataset Data Items for Transaction Type 12 (Manual Cash)[2]	b	Variable
3F8109	Unknown Proprietary Tag List (Mastercard) This is a constructed TLV that may contain “Unknown” Mastercard proprietary TLV data items. These are Mastercard data items that, as per Mastercard specs, have the properties: “IsKnown=False” and “IsPresent=True”.	b	Variable
FF8102	Tags to Write Before Gen AC	b	Variable
FF8103	Tags to Write After Gen AC	b	Variable
-	Disable *Data Exchange* for CL Mastercard See *Perform Transaction* command parameter for details.	-	-
-	Disable *Data Storage* for CL Mastercard See *Perform Transaction* command parameter for details.	-	-
See CL Terminal Config Data Items	All TLV data items from the contactless terminal configuration can also be defined in the MasterCard AID configuration. If a data item is defined in both contactless terminal configuration and in a MasterCard AID configuration, then the data item in the AID configuration will override the one in the terminal configuration.	*	*

[1] As per MasterCard Paypass M/Chip3 Spec, for MasterCard, the following data items are generic (terminal-specific) and not dataset-specific (per AID in our case).

- IFD Serial Number
- Terminal Country Code
- Transaction Currency Code
- Transaction Currency Exponent

[2] The MasterCard Paypass M/Chip 3 specification allows Dataset configurations to be defined that can be selected uniquely by referencing three parameters [Kernel + AID + Transaction Type]. As compared to this the older specifications only required per AID configurations. The Poynt Reader allows “virtual datasets” to be defined within an AID configuration for a Kernel if different values need to be set for one or more TLV data items for different Transaction Types. It does this via the four Poynt proprietary TLVs for “Virtual Datasets”

- Virtual Dataset Data Items for Transaction Type 00 (Purchase)
- Virtual Dataset Data Items for Transaction Type 01 (Cash Advance)
- Virtual Dataset Data Items for Transaction Type 09 (Purchase with Cashback)
- Virtual Dataset Data Items for Transaction Type 20 (Refund)

These “Virtual Datasets” allow for sub-configurations within an AID configuration that are Transaction-Type specific.

- If a data item is defined within a Virtual Dataset TLV for a specific Transaction Type, then this value

will override any values set for the data item in the AID configuration and in the contactless terminal configuration if the transaction performed has a matching transaction type.

- If a Virtual Dataset TLV is defined for the Transaction Type being performed, but does not have a particular data item defined within, then in that case the data item in the AID configuration will be used. And if that is not there either then the data item in the CL terminal configuration.
- Generally, when getting the value of a terminal resident data item from the configuration, the following will apply
    - Get the value from the TLV in CL Terminal Config (if present)
    - Override with the value from the TLV in AID Config (if present)
    - If the Virtual Dataset TLV for the current Transaction Type is present in the AID configuration, then override the value from the TLV encapsulated in the Virtual Dataset (if embedded TLV present)

So, for example, the following XML sequence (from a CC sample xml file) can be configured on a Poynt Reader using a Set AID Configuration command.

```
-<node name="APP1">
  -<map>
    <entry value="A0000000041010" key="<9F06>"/>
    <entry value="" key="<9F01>"/>
    <entry value="0002" key="<9F09>"/>
    <entry value="22" key="<9F35>[<009C>?00]"/>
    <entry value="14" key="<9F35>[<009C>?01]"/>
    <entry value="22" key="<9F35>[<009C>?09]"/>
    <entry value="22" key="<9F35>[<009C>?20]"/>
    <entry value="000000001000" key="<DF8126>[<009C>?00]"/>
    <entry value="000000020000" key="<DF8126>[<009C>!00]"/>
  </map>
</node>
```

The command data for the Set AID Configuration command is given below along with the same data parsed and with comments inserted. The portion that encodes the Virtual Datasets is given in green text.

Command Data:

```
01029F0607A00000000410109F01009F090200023F80000E9F350122DF8126060000000010003F
80010E9F350114DF8126060000000200003F80020E9F350122DF8126060000000200003F80030E
9F350122DF812606000000020000
```

Parsed Command Data:

```
01                              // Mode = Modify
02                              // Card Interface = Contactless AID
9F06 07 A0000000041010          // AID - Terminal
9F01 00                         // Acquirer ID
9F09 02 0002                    // App Version Number (Terminal)
3F8000 0E                       // Virtual Dataset for TT=00 (Purchase)
        9F35 01 22
        DF8126 06 000000001000
3F8001 0E                       // Virtual Dataset for TT=01 (Cash Advance)
        9F35 01 14
        DF8126 06 000000020000
3F8002 0E                       // Virtual Dataset for TT=09 (Purchase with Cashback)
        9F35 01 22
        DF8126 06 000000020000
3F8003 0E                       // Virtual Dataset for TT=20 Refund
        9F35 01 22
        DF8126 06 000000020000
```

3.5 Data Items specific to Contactless American Express AIDs (Kernel 4)

Tag	Data Item & Description	Format	Length (in Bytes)
1F8113*	Application Selection Indicator. Indicates whether the terminal should match the AID and AID Length in the card exactly or only up to the length of the AID in the terminal. Used if application selection using PPSE is not possible. Possible Values: 00 = Partial Selection Not Allowed. Must match full AID and length. 01 = Partial Selection Allowed. Default Value: Partial Selection Allowed	b	1
1F8119	AID Enabled	b	1
DF810C	Kernel ID Valid Value: 04h for CL American Express Kernel	b	1
1F8131	Configuration Version Version of the AID configuration for a contactless Amex AID. This is an optional field and can be used to store a version or a configuration identifier. The actual contents or format of this field are out of the scope of this document and should be defined at a higher level (Android or Server).	b	Variable
5F2A	Transaction Currency Code For CL this is a Terminal parameter for all Kernels but the sample configuration for Amex Kernel defines it as an AID parameter.	n3	2
9F09	Application Version Number (Terminal) Must be 0001 for AID ‘A0 00 00 00 25 01’	b	2
9F15	Merchant Category Code	n 4	2
9F16	Merchant Identifier	ans 15	15
9F1C	Terminal ID	8	an 8
9F33	Terminal Capabilities	b	3
9F35	Terminal Type	n2	1
9F4E	Merchant Name and Location	ans	Variable

<table>
<tr><th>Tag</th><th>Data Item & Description</th><th>Format</th><th>Length (in Bytes)</th></tr>
<tr><td>9F6D</td><td>For Amex XP 3.1: Contactless Reader Capabilities
Byte Format:
<table>
<tr><th>b7</th><th>b6</th><th>b5</th><th>b4</th><th>b3</th><th>b2</th><th>b1</th><th>b0</th><th>Description</th></tr>
<tr><td>0</td><td>0</td><td></td><td></td><td>0</td><td></td><td></td><td></td><td>Expresspay 1.0</td></tr>
<tr><td>0</td><td>0</td><td></td><td></td><td>1</td><td></td><td></td><td></td><td>RFU</td></tr>
<tr><td>0</td><td>1</td><td></td><td></td><td>0</td><td></td><td></td><td></td><td>Expresspay 2.0 Magstripe Only, or Expresspay ≥ 3.0 Magstripe – CVM Not Required</td></tr>
<tr><td>0</td><td>1</td><td></td><td></td><td>1</td><td></td><td></td><td></td><td>Expresspay ≥ 3.0 Magstripe – CVM Required</td></tr>
<tr><td>1</td><td>0</td><td></td><td></td><td>0</td><td></td><td></td><td></td><td>Expresspay 2.0 – EMV and Magstripe</td></tr>
<tr><td>1</td><td>0</td><td></td><td></td><td>1</td><td></td><td></td><td></td><td>RFU</td></tr>
<tr><td>1</td><td>1</td><td></td><td></td><td>0</td><td></td><td></td><td></td><td>Expresspay ≥ 3.0 EMV and Magstripe – CVM Not Required</td></tr>
<tr><td>1</td><td>1</td><td></td><td></td><td>1</td><td></td><td></td><td></td><td>Expresspay ≥ 3.0 EMV and Magstripe – CVM Required</td></tr>
</table>
For Amex XP 3.0: Expresspay Terminal Capabilities
Possible Values.
00h = Expresspay 1.0
40h = Expresspay 2.0 Magstripe only
48h = Expresspay 2.0 Magstripe – Mobile CVM Required
80h = Expresspay 2.0 EMV and Magstripe</td><td>n 2</td><td>1</td></tr>
<tr><td>9F6E</td><td>For Amex XP 3.1: Enhanced Contactless Reader Capabilities
For Amex XP 3.0: Terminal Transaction Capabilities

This field is formatted as follows (for both XP 3.0 and XP 3.1):
Byte 1:
Bit 7: AEIPS contact mode supported
Bit 6: Expresspay Magstripe Mode supported (Must be 1)
Bit 5: Expresspay EMV full online mode supported (Must be 0 for XP 3.1)
Bit 4: Expresspay EMV partial online mode supported
Bit 3: Expresspay Mobile Supported (Must be 1 for XP 3.0)
Bit 2-0: RFU (must always be set to 0)
Byte 2:
Bit 7: Mobile CVM supported
Bit 6: Online PIN supported
Bit 5: Signature
Bit 4: Plaintext Offline PIN
Bit 3-0: RFU (must always be set to 0)
Byte 3:
Bit 7: Terminal is offline only
Bit 6: CVM Required
Bit 5-0: RFU (must always be set to 0)
Byte 4:
Bit 7-0: RFU (must always be set to 0)</td><td>b</td><td>4</td></tr>
<tr><td>CFFFFF00</td><td>Data Record Tags (EMV)</td><td>b</td><td>Variable</td></tr>
<tr><td>CFFFFF01</td><td>Data Record Tags (MSD / Magstripe / Non-EMV)</td><td>b</td><td>Variable</td></tr>
</table>

Tag	Data Item & Description	Format	Length (in Bytes)
CFFFFF02	Select by AID Supported (Select via List of AIDs Supported?) Possible Values: 00h: Select by AID is not supported (Default). 01h: Select by AID is supported. 02h: Select by AID should only be performed if the condition is met (Amex XP 3.0). 03h: Select by AID should only be performed if the condition is met (Amex XP 3.1). For stops and comms failure Select by AID should not be performed.	b	1
CFFFFF03	Discretionary Data Tags (EMV)	b	Variable
CFFFFF04	Discretionary Data Tags (MSD / Magstripe / Non-EMV)	b	Variable
DF80FA	Unpredictable Number Range	b	?
DF80FB	Alternate Interface Supported		
DF80FC	Delayed Authorizations Supported	b	1
DF80FE	Online Capability 00h: (Or Absent): Delayed Authorization not enabled. 01h: Delayed Authorization is enabled.	b	1
DF8120	Terminal Action Code – Default (CL Only) (For CT it is E001)	b	5
DF8121	Terminal Action Code – Denial (CL Only) (For CT it is E02)	b	5
DF8122	Terminal Action Code – Online (CL Only) (For CT it is E002)	b	5
DFE2	Terminal Contactless Transaction Limit	b	4
DFE3	Terminal Contactless Floor Limit	b	4
DFE4	Terminal CVM Required Limit	b	4
E015	Threshold Value for Biased Random Selection Applies to: CT, CL	b	4
E013	Target Percentage to be used for Random Selection Applies to: CT, CL	b	4
E014	Maximum Target Percentage to be used for Biased Random Selection Applies to: CT, CL	b	4
DFFFDF4A	Amex Hold Time Value (for RF Field) Possible values are 10 - 30 Each unit signifies 100ms. Therefore, a value of 10-30 will allow setting up a hold time of 1000ms to 3000ms.	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
DFFFDF4D	CDA Issuer and ICC Public Key Recovery Step Possible Values: 00h: Issuer & ICC Public Key recovery will be performed before GEN AC. i.e. The reader detects CDA failure during Issuer or ICC public key recovery prior to the First Terminal Action Analysis. (Default) 01h: Issuer & ICC Public Key recovery will be performed after GEN AC. i.e. The reader detects CDA failure during Issuer or ICC public key recovery prior to the First Terminal Action Analysis. This parameter has no impact for SDA since for RSA, all RSA operations must still be performed by the Kernel before the first Gen AC. It only applies to CDA. Note: We should use the value 01h since this reduces the time the card needs to remain in the field, thus improving the Transaction Time.	b	1
DFFFDF47	DRL Reader Contactless Transaction Limit (Numeric)	n 12	6
DFFFDF48	DRL Reader Contactless Floor Limit (Numeric)	n 12	6
DFFFDF49	DRL Reader CVM Required Limit (Numeric)	n 12	6
DFFFDF4B	DRL Supported / DRL Enabled Possible Values: 00h: DRL Not Supported (Default) 01h: DRL Supported	b	1
DFFFDF4C	DRL Limit Set Value Possible Values: 00h – 0Fh: To match the DRL Set Value assigned by Amex. FFh: To indicate the Default DRL Set.	b	1

Here are some examples of how to set Dynamic Reader Limits (DRL) in the AID Configuration …

Example 1

```
<entry value="000000005500" key="<DFFFDF47>:01"/>
<entry value="000000010500" key="<DFFFDF48>:01"/>
<entry value="000000015500" key="<DFFFDF49>:01"/>
<entry value="01" key="<DFFFDF4B>"/>
<entry value="FF" key="<DFFFDF4C>:01"/>
```

Example 2

```
<entry value="000000005500" key="<DFFFDF47>:01"/>
<entry value="000000006000" key="<DFFFDF47>:02"/>
<entry value="000000010500" key="<DFFFDF48>:01"/>
<entry value="000000011000" key="<DFFFDF48>:02"/>
<entry value="000000015500" key="<DFFFDF49>:01"/>
<entry value="000000016000" key="<DFFFDF49>:02"/>
<entry value="01" key="<DFFFDF4B>"/>
<entry value="FF" key="<DFFFDF4C>:01"/>
<entry value="00" key="<DFFFDF4C>:02"/>
<entry value="01" key="<DFFFDF4D>"/>
```

3.6 Data Items specific to CL Discover DPAS & Zip AIDs (Kernel 6) (Amadis Kernel)

Tag	Data Item & Description	Format	Length (in Bytes)
1F8119	AID Enabled	b	1
DF810C	Kernel ID Valid Value: 06h for CL Discover Kernel	b	1
1F8131	Configuration Version Version of the AID configuration for a contactless Discover AID. This is an optional field and can be used to store a version or a configuration identifier. The actual contents or format of this field are out of the scope of this document and should be defined at a higher level (Android or Server).	b	Variable
5F2A	Transaction Currency Code Note: Preferably define this in CL Terminal Config	n 3	2
5F36	Transaction Currency Exponent Note: Preferably define this in CL Terminal Config	n 1	1
9F09	Application Version Number (Terminal) Possible Values: 0100h: AVN for Discover DPAS (If Amadis Kernel) 0200h: AVN for Discover ZIP (If Amadis Kernel)	b	2
9F1A	Terminal Country Code	n3	2
9F1B	Terminal Floor Limit	b	4
9F33	Terminal Capabilities	b	3
9F66	Terminal Transaction Qualifiers (TTQ)	b	4
CFFFFF00	Data Record Tags (EMV)	b	Variable
CFFFFF01	Data Record Tags (MSD / Magstripe / Non-EMV)	b	Variable
CFFFFF02	Select by AID Supported (Select via List of AIDs Supported?) Possible Values: 00h: Select by AID is not supported (Default). 01h: Select by AID is supported. 02h: Select by AID should only be performed if the condition is met (Amex XP 3.0). 03h: Select by AID should only be performed if the condition is met (Amex XP 3.1). For stops and comms failure Select by AID should not be performed.	b	1
CFFFFF03	Discretionary Data Tags (EMV)	b	Variable
CFFFFF04	Discretionary Data Tags (MSD / Magstripe / Non-EMV)	b	Variable
DF15	Merchant Category Code Note: The standard EMV Tag for Merchant Category Code is 9F15 but for some reason Discover specs use the tag DF15.	n 4	2

Tag	Data Item & Description	Format	Length (in Bytes)
DF1B	Kernel Configuration (Amadis Proprietary for CL Discover) Format: Bit 7: Exception List Supported Bit 6: Check PID Limit Bit 5: Extended Selection Supported Bit 4: Activate TAS 002 Bit 3: Do Not Fix Track Bit 2-0: RFU (must always be set to 0) Default Value: 20h	b	1
DF20	Terminal Action Code – Default (Amadis Proprietary) (CL Discover) For Contact EMV, and other CL Kernels, different Tags are used. Default Value: 0000000000h	b	5
DF21	Terminal Action Code – Denial (Amadis Proprietary) (CL Discover) For Contact EMV, and other CL Kernels, different Tags are used. Default Value: 0000000000h	b	5
DF22	Terminal Action Code – Online (Amadis Proprietary) (CL Discover) For Contact EMV, and other CL Kernels, different Tags are used. Default Value: 0000000000h	b	5
DF30	Bitmap Entry Point (Amadis Proprietary for CL Discover) Format: Bit 7: Status Check Support Flag Bit 6: Zero Amount Allowed Flag Bit 5: RCTL Bit 4: RCFL Bit 3: RCRL Bit 2-0: RFU (must always be set to 0) Default Value: 38h	b	1
DF32	Status Zero Amount Allowed Flag (Amadis Proprietary for CL Discover) Possible Values: 01h: Option 1 = Online Cryptogram Request Other: Not Allowed	b	1
DF23	Terminal (Reader) Contactless Floor Limit (Amadis Proprietary) See Appendix A.26 *Configuring CL Pre-Processing Tags for Multi-Vendor Kernels*.	n12	6
DF24	Terminal (Reader) Contactless Transaction Limit (Amadis Proprietary) See Appendix A.26 *Configuring CL Pre-Processing Tags for Multi-Vendor Kernels*.	n12	6
DF26	Terminal (Reader) Contactless CVM Required Limit (Amadis Proprietary) See Appendix A.26 *Configuring CL Pre-Processing Tags for Multi-Vendor Kernels*.	n12	6
DF70	Loyalty program ID Possible Values: 10h – 1Fh 20h – 2Fh 30h – 3Fh	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
DF71	Value Added Tax 1 This is the value added tax rate. For example, a value added tax of 5.88% will be coded as 0588h.	n 4	2
DF72	Value Added Tax 2	n 4	2
DFE1	Status Check Supported	b	1
DFE5	Zero Amount Allowed 00h: Zero amount transactions are not supported. 01h: Zero amount transactions are supported.	b	1
DFEF	Extended Selection Support	b	1
DFFFDF02	Reader Contactless Transaction Limit (CC Proprietary)(Entry Point) See Appendix A.26 *Configuring CL Pre-Processing Tags for Multi-Vendor Kernels*.	n 12	6
DFFFDF03	Reader Contactless Floor Limit (CC Proprietary) (Entry Point) See Appendix A.26 *Configuring CL Pre-Processing Tags for Multi-Vendor Kernels*.	n 12	6
DFFFDF04	Reader Contactless CVM Limit (CC Proprietary) (Entry Point) See Appendix A.26 *Configuring CL Pre-Processing Tags for Multi-Vendor Kernels*.	n 12	6

3.7 Data Items specific to Contactless Interac AIDs (Kernel 3E)

Tag	Data Item & Description	Format	Length (in Bytes)
1F8119	AID Enabled	b	1
DF810C	Kernel ID Valid Value: 3Eh for CL Interac Kernel. Note: Since Interac does not have an EMV sanctioned Kernel ID, using a Poynt-specified Kernel ID. Each time EMV Co releases a new spec or a new list of Kernel IDs, we should make sure there is no conflict. If there is, we will have to change Interac's Kernel ID to another unused value or if Interac have gotten a proper Kernel ID value from EMVCo, then use that one.	b	1
1F8131	Configuration Version Version of the AID configuration for a contactless Interac AID. This is an optional field and can be used to store a version or a configuration identifier. The actual contents or format of this field are out of the scope of this document and should be defined at a higher level (Android or Server).	b	Variable
CFFFFF00	Data Record Tags (EMV)	b	Variable
CFFFFF02	Select by AID Supported (Select via List of AIDs Supported?) Possible Values: 00h: Select by AID is not supported (Default). 01h: Select by AID is supported. 02h: Select by AID should only be performed if the condition is met (Amex XP 3.0). 03h: Select by AID should only be performed if the condition is met (Amex XP 3.1). For stops and comms failure Select by AID should not be performed.	b	1
9F09	Application Version Number (Terminal)	b	2
9F1B	Terminal Floor Limit	b	4
9F33	Terminal Capabilities Note: Used to populate Interac Tag 9F59. Format: Byte 1: Bit 7: Manual Key Entry Bit 6: Magnetic Stripe Bit 5: IC with Contacts Bits 4-0: RFU (must be set to all 0's) Byte 2: Bit 7: Plaintext PIN for Offline Verification Bit 6: Enciphered PIN for Online Verification Bit 5: Signature Bit 4: Enciphered PIN for Offline Verification Bit 3: No CVM Required Bit 2-0: RFU (must be set to all 0's) Byte 3: Bit 7: SDA Bit 6: DDA Bit 5: Card Capture Bit 4: RFU (must always be set to 0) Bit 3: CDA Bit 2-0: RFU (must be set to all 0's)	b	3

Tag	Data Item & Description	Format	Length (in Bytes)
9F40	Additional Terminal Capabilities Note: Used to populate CL Interac Tag 9F59.	b	5
9F58	Merchant Type Indicator (CL Interac) This tag provides Merchant type Indicator that is used by the card for its card risk management – 5 values are possible: 01, 02, 03 04 and 05.	n1	1
9F59	Terminal Transaction Information (TTI) (CL Interac) Terminal information for current transaction. Note: Do NOT define this in the config. It is created by the kernel from the tags 9F33, 9F40, DF1B. Format: Byte 1: Bit 7: Reader with Display Capability Bit 6: Interac Contact Application Available Bit 5: Interac Contact Application at other Terminal Bit 4: CDA Supported Bit 3: Offline Capable Terminal (0 means Online-Only Terminal) Bit 2: Online PIN Supported Bit 1: RFU (must be set to 0) Bit 0: RFU (must be set to 0) Byte 2: Bits 7,6: Input Capabilities. 00: Contactless Only Capable 01: Contactless & MSR Capable 10: Contactless, Contact Chip & MSR Capable 11: Contactless & Contact Chip Capable Bit 5: RFU (must be set to 0) Bit 4: RFU (must be set to 0) Bit 3: RFU (must be set to 0) Bit 2: Mobile NFC Device (FFI=03) accepted Bit 1: Contactless Card (FFI=00,01,02) accepted Bit 0: Always set to 1. Indicates acceptance data present in this version of TTI. Byte 3: Bits 7-0: RFU (all bits must be set to 0)	b	3
9F5F	Terminal (Reader) Contactless Floor Limit (CL Interac) Floor Limit Amount used to compare against Transaction Amount	n12	6
9F5D	Terminal Contactless Receipt Required Limit (CL Interac) Limit Amount used to compare against Transaction amount to automatically print a transaction record.	n12	6
9F5E	Terminal Option Status (TOS) (CL Interac) Terminal supported options. Format: Byte 1 Bit 7: Use other Interface if different Currency Bit 6: Use other Interface if different Country Code Bit 5: Use other Interface if domestic transaction with different Currency. Bit 4: RFU (must be set to 0) Bit 3: RFU (must be set to 0) Bit 2: RFU (must be set to 0) Bit 1: RFU (must be set to 0) Bit 0: RFU (must be set to 0) Byte 2: Bits 7-0: RFU (all bits must be set to 0)	b	2

Tag	Data Item & Description	Format	Length (in Bytes)
5F2A	Transaction Currency Code Note: Preferably define this in CL Terminal Config	n3	2
5F36	Transaction Currency Exponent Note: Preferably define this in CL Terminal Config	n1	1
DF1B	Kernel Configuration (Amadis Proprietary for CL Interac) Note: Used to populate Interac Tag 9F59 and the Retry Limit. Byte 1: Interac Retry Limit (Interac) Default value for the total number of tap attempts during an Interac Mobile Debit (NFC) application transaction. Format: n1 Byte 2: Bit 7: Interac Contact Bit 6: Interac on other Terminal Bit 5: Mobile NFC Bit 4: CL Card Bit 3: Legacy Floor Limit Bit 2: Always DD Bit 1: Flash Terminal v1.4 Bit 0: RFU (must be set to 0)	b	2
DF20	Terminal Action Code – Default (Amadis Proprietary) (CL Interac) For Contact EMV, and other CL Kernels, different Tags are used.	b	5
DF21	Terminal Action Code – Denial (Amadis Proprietary) (CL Interac) For Contact EMV, and other CL Kernels, different Tags are used.	b	5
DF22	Terminal Action Code – Online (Amadis Proprietary) (CL Interac) For Contact EMV, and other CL Kernels, different Tags are used.	b	5
DF2D	Message Hold Time (Amadis Proprietary) Expressed in units of 100ms.	b	3
DF6E	Threshold Value for Biased Random Selection Value used in terminal risk management for random transaction selection. This value must be zero or a positive number less than the floor limit. Binary in units of currency (cents, etc.). For Contact EMV, and other CL Kernels, different Tags are used.	b	3
DF6F	Maximum Target Percentage to be used for Biased Random Selection Value used in terminal risk management for random transaction selection. Possible values are in the range of 0 to 99 but at least as high as Target Percentage to be Used for Random Selection. This is the desired percentage of transactions ‘just below’ the floor limit that will be selected by this algorithm. Example: 15% will be encoded as 0F hex. For Contact EMV, and other CL Kernels, different Tags are used.	b	1
DF70	Target Percentage to be used for Random Selection Value used in terminal risk management for random transaction selection. Possible values are in the range of 0 to 99. Example: 15% will be encoded as 0F hex. For Contact EMV, and other CL Kernels, different Tags are used.	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
1F8167	Optimize for Performance For Interac, this parameter can be used to bypass sending the “Processing” UI Notification. The default value for this parameter is 00h This parameter should only be used (i.e. set to 01h) for Performance Testing. It should not be used for Certification Testing and in Production units.	b	1
1F816F	Enforce MAC The format of this data item is as follows: Byte 1: Bit 7-2: RFU (must always be set to 0) Bit 1: Interac Safe-T Enabled Bit 0: Enforce Interac MACing on this AID	b	Variable (Max 4)

3.8 Data Items specific to Contactless Bancomat AIDs (Kernel 3D)

Tag	Data Item & Description	Format	Length (in Bytes)
1F8119	AID Enabled	b	1
DF810C	Kernel ID Valid Value: 3Dh for CL Bancomat Kernel. Note: Since Bancomat does not have an EMV sanctioned Kernel ID, using a Poynt-specified Kernel ID. Each time EMV Co releases a new spec or a new list of Kernel IDs, we should make sure there is no conflict. If there is, we will have to change Bancomat's Kernel ID to another unused value or if Bancoat have gotten a proper Kernel ID value from EMVCo, then use that one.	b	1
1F8131	Configuration Version Version of the AID configuration for a contactless Bancomat AID. This is an optional field and can be used to store a version or a configuration identifier. The actual contents or format of this field are out of the scope of this document and should be defined at a higher level (Android or Server).	b	Variable
CFFFFF00	Data Record Tags (EMV)	b	Variable
CFFFFF02	Select by AID Supported (Select via List of AIDs Supported?) Possible Values: 00h: Select by AID is not supported (Default). 01h: Select by AID is supported. 02h: Select by AID should only be performed if the condition is met (Amex XP 3.0). 03h: Select by AID should only be performed if the condition is met (Amex XP 3.1). For stops and comms failure Select by AID should not be performed.	b	1
9F09	Application Version Number (Terminal)	b	2
DF1B	Kernel Configuration (Amadis Proprietary for CL Bancomat) Byte1 Bit 7: Extended Selection Flag Supported Bit 6: PROCESSING Message Disabled Bit 5: Always DD Bit 4: RFU (must always be set to 0) Bit 3: Ask for PIN from L3 Bit 2: RFU (must always be set to 0) Bit 1: RFU (must always be set to 0) Bit 0: EMVCo Entry Point Byte2 Bit 7-0: Online Retry Counter	b	2
DF20	Terminal Action Code – Default (Amadis Proprietary) (CL Bancomat) For Contact EMV, and other CL Kernels, different Tags are used.	b	5
DF21	Terminal Action Code – Denial (Amadis Proprietary) (CL Bancomat) For Contact EMV, and other CL Kernels, different Tags are used.	b	5
DF22	Terminal Action Code – Online (Amadis Proprietary) (CL Bancomat) For Contact EMV, and other CL Kernels, different Tags are used.	b	5

Tag	Data Item & Description	Format	Length (in Bytes)
DF23	Terminal (Reader) Contactless Floor Limit (Amadis Proprietary) Floor Limit Amount used to compare against Transaction Amount	n12	6
DF24	Terminal (Reader) Contactless Transaction Limit (Amadis Proprietary)	n12	6
DF26	Terminal (Reader) Contactless CVM Required Limit (Amadis Proprietary)	n12	6
DF71	Terminal Action Code – Switch Interface (Amadis Proprietary) (CL Bancomat) For other CL Kernels, different Tags are used.	b	5

3.9 Data Items specific to Contactless JCB AIDs (Kernel 5)

Tag	Data Item & Description	Format	Length (in Bytes)
1F8119	AID Enabled	b	1
DF810C	Kernel ID Valid Value: 05h for CL JCB Kernel.	b	1
1F8131	Configuration Version Version of the AID configuration for a contactless JCB AID. This is an optional field and can be used to store a version or a configuration identifier. The actual contents or format of this field are out of the scope of this document and should be defined at a higher level (Android or Server).	b	Variable
CFFFFF00	Data Record Tags (EMV)	b	Variable
CFFFFF02	Select by AID Supported (Select via List of AIDs Supported?) Possible Values: 00h: Select by AID is not supported (Default). 01h: Select by AID is supported. 02h: Select by AID should only be performed if the condition is met (Amex XP 3.0). 03h: Select by AID should only be performed if the condition is met (Amex XP 3.1). For stops and comms failure Select by AID should not be performed.	b	1
5F2A	Transaction Currency Code Note: Preferably define this in CL Terminal Config	n 3	2
5F36	Transaction Currency Exponent Note: Preferably define this in CL Terminal Config	n 1	1
9F1A	Terminal Country Code	n 3	2
9F1B	Terminal Floor Limit	b	4
9F33	Terminal Capabilities Byte1: Bit 7: Manual key entry Bit 6: Magnetic stripe Bit 5: IC with contacts Bit 4-0: RFU (must always be set to 0) Byte2: Bit 7: Plaintext PIN for ICC verification Bit 6: Enciphered PIN for online verification Bit 5: Signature (paper) Bit 4: Enciphered PIN for offline verification Bit 3: No CVM Required Bit 2-0: RFU (must always be set to 0) Byte3: Bit 7: SDA Bit 6: DDA Bit 5: Card capture Bit 4: RFU (must always be set to 0) Bit 3: CDA Bit 2-0: RFU (must always be set to 0) Default value: 6B0080h	b	3
9F52	Terminal Compatibility Indicator	b	1

Tag	Data Item & Description	Format	Length (in Bytes)
9F53	Terminal Interchange Profile (Synthetic Tag Calculated at Run Time). Terminal Interchange Profile (TIP) is a special tag which is calculated during the run time based on the terminal capabilities (9F33) tag and kernel configuration (DF1B) tag for Amadis kernel. It defines the reader CVM requirement and capabilities, as well as other reader capabilities (online capability, contact EMV capability) for the Transaction. Byte1: Bit 7: CVM required by reader / N/A Bit 6: Signature supported (9F33: B3b5) Bit 5: Online PIN supported (9F33: B2b6) Bit 4: On-device CVM supported (DF1B: B3b7) Bit 3: RFU (must always be set to 0) Bit 2: Reader is a Transit Reader (DF1B: B3b6) Bit 1: EMV contact chip supported (9F33: B1b5) Bit 0: (Contact chip) Offline PIN supported (9F33: (B2b7 & B2b4)) Byte2: Bit 7: Issuer Update supported (DF1B: B3b5) Bit 6-0: RFU (must always be set to 0) Byte3: Bit 7-0: RFU (must always be set to 0)	b	3
9F66	Terminal Transaction Qualifiers (TTQ)	b	4
DF1B	Kernel Configuration (Amadis Proprietary for CL JCB) Byte 1: (Reflects Combination Options) Bit 7: RFU (must always be set to 0) Bit 6: Status Check Supported Bit 5: ODA Supported Bit 4: Exception File Supported Bit 3: Random Transaction Selection Supported Bit 2: RFU (must always be set to 0) Bit 1: EMV Mode Supported Bit 0: Legacy Mode Supported Byte 2: (Reflects Combination Options) Bit 7-0: RFU (must always be set to 0) Byte 3: Bit 7: On Device CVM Bit 6: Transit Reader Supported Bit 5: Issuer Update Supported Bit 4-1: RFU (must always be set to 0) Bit 0: TVR with Online PIN for Legacy Default value: 6B0080h	b	3
DF1C	Max Lifetime Torn Transaction(s) (Amadis Proprietary) Default Value: 003Ch	b	2
DF1D	Torn Depth (Amadis Proprietary) Default Value: 01h	b	1
DF20	Terminal Action Code – Default (Amadis Proprietary) For Contact EMV, and other CL Kernels, different Tags are used. Default value: 0000000000 h	b	5
DF21	Terminal Action Code – Denial (Amadis Proprietary) For Contact EMV, and other CL Kernels, different Tags are used. Default value: 0000000000 h	b	5

Tag	Data Item & Description	Format	Length (in Bytes)
DF22	Terminal Action Code – Online (Amadis Proprietary) For Contact EMV, and other CL Kernels, different Tags are used. Default value: 0000000000 h	b	5
DF23	Reader Contactless Floor Limit (Amadis Proprietary)	n12	6
DF24	Reader Contactless Transaction Limit (Amadis Proprietary)	n12	6
DF26	Reader Contactless CVM Required Limit (Amadis Proprietary)	n12	6
DF2D	Message Hold Time (Amadis Proprietary) Expressed in units of 100ms.	b	3
DFEF	Extended Selection Support	b	1
DFFFDF02	Reader Contactless Transaction Limit (CC Proprietary)(Entry Point) See Appendix A.26 *Configuring CL Pre-Processing Tags for Multi-Vendor Kernels*.	n 12	6
DFFFDF03	Reader Contactless Floor Limit (CC Proprietary) (Entry Point) See Appendix A.26 *Configuring CL Pre-Processing Tags for Multi-Vendor Kernels*.	n 12	6
DFFFDF04	Reader Contactless CVM Limit (CC Proprietary) (Entry Point) See Appendix A.26 *Configuring CL Pre-Processing Tags for Multi-Vendor Kernels*.	n 12	6

3.10 Data Items specific to Contactless CUP AIDs (Kernel 7)

Tag	Data Item & Description	Format	Length (in Bytes)
1F8119	AID Enabled	b	1
DF810C	Kernel ID Valid Value: 07h for CL CUP International Kernel.	b	1
1F8131	Configuration Version Version of the AID configuration for a contactless CUP AID. This is an optional field and can be used to store a version or a configuration identifier. The actual contents or format of this field are out of the scope of this document and should be defined at a higher level (Android or Server).	b	Variable
CFFFFF00	Data Record Tags (EMV)	b	Variable
CFFFFF02	Select by AID Supported (Select via List of AIDs Supported?) Possible Values: 00h: Select by AID is not supported (Default). 01h: Select by AID is supported. 02h: Select by AID should only be performed if the condition is met (Amex XP 3.0). 03h: Select by AID should only be performed if the condition is met (Amex XP 3.1). For stops and comms failure Select by AID should not be performed.	b	1
5F2A	Transaction Currency Code Note: Preferably define this in CL Terminal Config	n 3	2
5F36	Transaction Currency Exponent Note: Preferably define this in CL Terminal Config	n 1	1
9F09	Application Version Number (Terminal)	b	2
9F1A	Terminal Country Code	n 3	2
9F1B	Terminal Floor Limit Only applicable when Terminal Contactless Floor Limit is absent.	b	4

Tag	Data Item & Description	Format	Length (in Bytes)
9F33	Terminal Capabilities Byte1: Bit 7: Manual key entry Bit 6: Magnetic stripe Bit 5: IC with contacts (should match 9F66 B1b5) Bit 4-0: RFU (must always be set to 0) Byte2: Bit 7: Plaintext PIN for ICC verification (should match 9F66 B3b6) Bit 6: Enciphered PIN for online verification (should match 9F66 B1b2) Bit 5: Signature (paper) Bit 4: Enciphered PIN for offline verification Bit 3: No CVM Required (should match 9F66 B2b6) Bit 2-0: RFU (must always be set to 0) Byte3: Bit 7: SDA Bit 6: DDA Bit 5: Card capture Bit 4: RFU (must always be set to 0) Bit 3: CDA Bit 2-0: RFU (must always be set to 0)	b	3
9F40	Additional Terminal Capabilities	b	5
9F66	Terminal Transaction Qualifiers (TTQ) Byte 1: Bit 7: RFU (must always be set to 0) Bit 6: Full Transaction Flow Supported Bit 5: EMV Mode Supported (should match 9F33 B1b5) Bit 4: Full transaction flow in contact Support Bit 3: Offline-only terminal Bit 2: Online PIN Supported (should match 9F33 B2b6) Bit 1: Signature Supported (should match 9F33 B2b5) Bit 0: ODA for Online Auth supported. Byte 2: Bit 7: Request Online cryptogram Bit 6: CVM Requested (should match 9F33 B2b3) Bit 5-0: RFU (must always be set to 0) Byte 3: Bit 7: RFU (must always be set to 0) Bit 6: Consumer Device CVM Supported (should match 9F33 B2b7) Bit 5-0: RFU (must always be set to 0) Byte 4: Bit 7: fDDA v1.0 Supported Bit 6-0: RFU (must always be set to 0)	b	4

Tag	Data Item & Description	Format	Length (in Bytes)
DF1B	Kernel Configuration (Amadis Proprietary for CL CUP International) Byte 1: (Reflects Combination Options) Bit 7-0: RFU (must always be set to 0) Byte 2: (Reflects Combination Options) Bit 7: C7 Outcome Bit 6: TVR Not Reset Bit 5: 9F27 Always Raised Bit 4: Not Forced Online Bit 3: Standard UICS DT/CT Application Flow Bit 2: Always DD Bit 1: Not Decline on Transit Debit AID ONLINE PIN Case Bit 0: Transit Terminal	b	2
DF1C	Max Lifetime Torn Transaction(s) (Amadis Proprietary)	b	2
DF1D	Torn Depth (Amadis Proprietary)	b	1
DF20	Terminal Action Code – Default (Amadis Proprietary) (CL CUP) For Contact EMV, and other CL Kernels, different Tags are used.	b	5
DF21	Terminal Action Code – Denial (Amadis Proprietary) (CL CUP) For Contact EMV, and other CL Kernels, different Tags are used.	b	5
DF22	Terminal Action Code – Online (Amadis Proprietary) (CL CUP) For Contact EMV, and other CL Kernels, different Tags are used.	b	5
DF23	Reader Contactless Floor Limit (Amadis Proprietary)	n12	6
DF24	Reader Contactless Transaction Limit (Amadis Proprietary)	n12	6
DF26	Reader Contactless CVM Required Limit (Amadis Proprietary)	n12	6
DF2D	Message Hold Time (Amadis Proprietary) Expressed in units of 100ms.	b	3
DF30	Bitmap Entry Point (Amadis Proprietary for CL CUP) Format: Bit 7: Status Check Support Flag Bit 6: Zero Amount Allowed Flag Bit 5: RCTL Bit 4: RCFL Bit 3: RCRL Bit 2-0: RFU (must always be set to 0)	b	1
DF32	Status Zero Amount Allowed Flag (Amadis Proprietary for CL CUP) Possible Values: 01h: Option 1 = Online Cryptogram Request Other: Not Allowed	b	1
DFEF	Extended Selection Support	b	1
DFFFDF02	Reader Contactless Transaction Limit (CC Proprietary)(Entry Point) See Appendix A.26 *Configuring CL Pre-Processing Tags for Multi-Vendor Kernels*.	n 12	6
DFFFDF03	Reader Contactless Floor Limit (CC Proprietary) (Entry Point) See Appendix A.26 *Configuring CL Pre-Processing Tags for Multi-Vendor Kernels*.	n 12	6
DFFFDF04	Reader Contactless CVM Limit (CC Proprietary) (Entry Point) See Appendix A.26 *Configuring CL Pre-Processing Tags for Multi-Vendor Kernels*.	n 12	6

4 CA Public Key Configuration

This configuration data is to load EMV CA Public Keys with the specified RID and Index into the Reader, checks the validity of the key and if the validity check passes, it stores it in non-volatile storage.

Format of the Key Data is given in the following Table.

Parameter	Field	Length (in Bytes)	Description
cardInterface	Interface	1	Card Interfaces for which this Key can be used Bit 0: Contactless Interface 0: Cannot be used for the CL interface. 1: Can be used for the CL interface. Bit 1: Contact Interface 0: Cannot be used for the CT interface. 1: Can be used for the CT interfa
rid	RID	5	Registered ID ff the Key being loaded
keyIndex	KeyIndex	1	Index of the Key being loaded
hashAlgorithmIndicator	CA Hash Algorithm Indicator	1	Certification Authority Hash Algorithm to produce hash result in digital signature scheme. 01h = SHA1
publicKeyAlgorithmIndicator	CA Public Key Algorithm Indicator	1	Certification Authority Algorithm to sign the key certificates. 01h = RSA
publicKeyChecksum	CA Public Key Checksum	20	Checksum/Hash calculated using SHA-1 over the fields specified by EMV Book 2 (i.e. RID, Key Index, Modulus & Exponent). The length of the exponent used to generate the SHA-1 Hash should be the actual length as would be reported by any PICC (i.e.1 or 3 bytes) and not the fixed 4-byte length.
publicKeyExponent	CA Public Key Exponent	4 (PICC-based length will be 1 or 3)	Certification Authority Public Key Exponent as a 32-bit, big-endian number. The real length of the exponent will always be 1 or 3 (corresponing to the two possible values it may have i.e. 1 or 65537). When calculating the checksum to validate the key being loaded,the real length of the exponent must be used.
publickeyModulus	CA Public Key Modulus	Variable	CA Public Key Modulus

5 Revocation List Configuration

The format of the Revocation List Entry parameters is

Parameter	Field	Length (in Bytes)	Description
rid	RID	5	The Registered ID associated with the Revocation List Entry. Format: Binary Example: A0 00 00 00 04 hex
keyIndex	Index	1	The CA Public Key Index associated with the Revocation List Entry. Format: Binary Example: 05h
certSerialNumber	Certificate Serial Number	3	The Certificate Serial Number for the Issuer Public Key Certificate. Format: Binary Example: 002597h

6 Exception List Configuration

The format of the Exception List Entry data is

Parameters	Field	Length (in Bytes)	Description
pan	PAN	10	The blacklisted Primary Account Number (PAN), right-padded with Fh. Format: Compressed Numeric (cn) 19 nibbles (10 bytes) Example: 3451582273680285320F (a 19-digit PAN) Example: 345158227368028 5FFFF (a 16-digit PAN)
sequenceNumber	Sequence Number	1	The Sequence Number Format: Binary Example: 25h

Appendices

Appendix A.1: References

https://www.emvco.com/wp-content/uploads/2017/05/EMV_v4.3_Book_3_Application_Specification_20120607062110791.pdf

Appendix A.2: Proprietary TLV Tags used by Poynt (Primitive Tags)

A list of proprietary TLV tags that Poynt has used to define primitive data items that do not have Tags in the standard Contact and Contactless EMV specifications or in the card association specific contactless specifications is given in the following table.

Tag	Name	Format	Length of TLV Value (in Bytes)
DFD8	Online Result	b	1
1F8100	This is not a valid tag as per BER TLV Rules	-	-
1F8101	Key Serial Number (KSN) for Encrypted PIN	b	5-10
1F8102	Key Serial Number (KSN) for Encrypted Data	b	5-10
1F8103	First Clear PAN Digits	an	6
1F8104	Last Clear PAN Digits	an	4
1F8106	PAN Hash	b	32
1F8107	Cardholder Confirmation Supported	b	1
1F8108	Application Index	b	1
1F8109	Cardholder Confirmation Required	b	1
DFD6 ~~1F810F~~	Advice Supported	b	1
1F8110	Force Terminal Risk Management	b	1
1F8111	Recommended CDA Processing	b	4
1F8112	Decline on Comms Fail	b	1
1F8113	Application Selection Indicator	b	1

Tag	Name	Format	Length of TLV Value (in Bytes)
1F8114	PIN Bypass Supported	b	1
1F8115	Enable Certification Log Event Notifications	b	1
~~1F8116~~ DFD9	Authorization Response Code (ARC) Referral	an	2
1F8117	Online PIN for TTQ Override	b	1
1F8118	Signature for TTQ Override	b	1
1F8119	AID Enabled	b	1
1F8120	Use Alternate Advice Logic	b	1
1F8121	Merchant Forced Acceptance	b	1
1F8122	CT to MSR Fallback Configuration	b	3
1F8123	Allow MSR transaction on Chip Card (without Fallback)	b	1
1F8124	Delayed Authorization Supported	b	1
1F8124	Delayed Authorization Required	b	1
1F8125	Visa Apps Supported	b	1
1F8126	Force Online Authorization	b	1
1F8127	PCI Key Management Scheme for PIN Encryption	b	1
1F8128	PCI Key Management Scheme for Data Encryption	b	1
1F8129	Data Format for Data Encryption	b	1
1F812A	CT EMV Special Flow	b	2
1F812B	BIN Range	an	6
1F812C	Session Key ID for Encrypted PIN	b	8
1F812D	Session Key ID for Encrypted Data	b	8
1F812E	Stop after read records Special Flow Timeout	b	2
1F812F	Custom BIN Range List	b	Variable (Max 128)
1F8130	Terminal Supported Languages	an2	Variable
1F8131	Configuration Version	b	Variable

Tag	Name	Format	Length of TLV Value (in Bytes)
1F8132	Auto-Detect MSR Debit	b	1
1F8133	Track Data Format 2	b	1
1F8134	Input Field List	b	Variable
1F8135	Output Field List	b	Variable
1F8136	Electronic Referral Content	b	Variable
1F8137	Positive ID Content	b	Variable
1F8138	Electronic Referral	b	8
1F8139	Positive ID	b	8
1F813A	Card Security Code (CSC/CVV/CVC/CID/CAV2/ CVC2/CVV2)	b	Variable
1F813B	Birth Year	n4	2
1F813C	Birth Month	n2	1
1F813D	Birth Day	n2	1
1F813E	CNPJ	n	Variable
1F813F	Client Code	n	Variable
1F8140	Invoice	n	Variable
1F8141	CPF Number	n	Variable
1F8142	RG Number	n	Variable
1F8143	Last 4 CPF Digits	n	Variable
1F8144	Last 4 RG Digits	n	Variable
1F8145	Age	n	Variable
1F8146	Dia Venc Fatura	n	Variable
1F8147	Zip Code (Residential)	n	Variable
1F8148	Zip Code (Commercial)	n	Variable
1F8149	Expiry Month	n	Variable
1F814A	Expiry Year	n	Variable
1F814B	Current CTA	n	Variable
1F814C	Agency Code	n	Variable
1F814D	Phone (Residence)	n	Variable
1F814E	Phone (Work)	n	Variable
1F814F	Phone (Cell)	n	Variable
1F8150	Stan (Last 4 Digits)	n4	2
1F8151	Track 1 Length	b	1
1F8152	Password	n	Variable
1F8153	MSR Transaction Token	b	4
1F8154	Terminal Configuration Checksum	b	4

Tag	Name	Format	Length of TLV Value (in Bytes)
1F8155	Select DUKPT PIN Encryption Key Slot	b	1
1F8156	Select DUKPT Data Encryption Key Slot	b	1
1F8157	Select M/S PIN Encryption Key Slot	b	1
1F8158	Select M/S Data Encryption Key Slot	b	1
1F8159	ADA-Compliant Keypad	b	1
1F815B			
1F815C	Elavon Manual Card Data	b	Variable
1F815D	Track 1 Digits (In Unencrypted Track 1)	b	1
1F815E	Track 2 Digits (In Unencrypted Track 2)	b	1
1F815F	Track1 Left-Padding Digits	b	1
1F8160	Track 2 Left-Padding Digits	b	1
1F8161	Track1 Right-Padding Digits	b	1
1F8162	Track 2 Right-Padding Digits	b	1
1F8163	CT Interac Config	b	1
1F8164	Always Send App Selection Required for CT	b	1
1F8165	Receipt Required	b	1
1F8166	Screen Orientation	b	1
1F8167	Optimize for Performance	b	1
1F8168	Poynt Stan (For Interac MAC)	n6	3
1F8169	Processing Code (For Interac MAC) See also Tag 1F8178.	n6	3
1F816A	Interac MAC (Terminal) (For Interac MAC)	b	4
1F816B	Interac MAC (Host) (For Interac MAC)	b	4
1F816C	Host Stan (For Interac MAC)	n6	3
1F816D	Debit Response Code (For Interac MAC)	an	2
1F816E	Retrieval Reference Number (For Interac MAC)	an	12

Tag	Name	Format	Length of TLV Value (in Bytes)
1F816F	Enforce MAC	b	Variable Max: 4
1F8170	MSR Track Standards Config	b	1
1F8171	PIN Entry UI Config	b	1
1F8172	UID / Serial Number	b	Variable Max:10
1F8173	ATR (Answer to Reset)	b	Variable
1F8174	C-APDU	b	Variable
1F8175	R-APDU	b	Variable
1F8176	APDU OK Condition	b	Variable
1F8177	Flush MSR Data before Start of Transaction	b	1
1F8178	Processing Code (Alternate) (For Interac MAC) See also Tag 1F8169	n6	3
1F8179	Reversal Reason	Out of scope	Out of scope of this doc
1F817B	Switch from CL to CT Interface on Card Insert	b	1
1F817C	Enable Touch During Transactions	b	1
1F817D	Bypass CA Public Key Validation during Key Load	b	1
1F817E	UI Code	b	4
1F817F	Mock Transaction	b	1
1F8180-1F81FF	Don't Use - This is not a valid 3-byte tag as per BER TLV Rules. This indicates a 4th Tag Byte.	-	-
1F8200	Don't Use	-	-
1F8207	CL EMV Special Flow	b	1
1F8208	Combined Track Data (Part 1)	b	
1F8209	Combined Track Data (Part 2)	b	
1F820A	PCI Key Management Scheme for Data MAC	b	1

Tag	Name	Format	Length of TLV Value (in Bytes)
1F820B	KSN for Data MAC Generation/Verification	b	5-10
1F820C			
1F8220	Terminal Behavior on Missing PIN Key	b	1
1F8221	MSR Flow Config	b	1
1F8222	Track Status	b	1
1F8223	MSR Flow Decision	b	1
1F8224	Terminal Capabilities CVM Override	b	1
1F8225	Fallback from CL to Other Interface	b	1
1F8226	Terminal Behavior on PIN Timeout	b	1
1F8227	Outcome Parameter Set Format	b	1
1F8228	Use JCB Parsing	b	1
1F8229	PPSE DF Name Optional	b	1
1F822A	CT to MSR Fallback Reason Code	b	1
1F822B	Multiple Application Version Numbers (Terminal)	b	Variable (Max: 20)
1F822C	MSR Flags	b	1
1F8230	RNIB Features	b	1
1F8231	Scheme ID	b	1
1F8232	PIN Entry Result	b	1
1F8233	Wakeup on Touch	b	2
1F8233	Manufacturing ID	b	
1F8234	Enable/Disable Enhanced Firmware Logging	b	1
1F8225 - 1F827F	Next series available		
1F8280	Don't Use - This is not a valid 3-byte tag as per BER TLV Rules. This indicates a 4th Tag Byte.	-	-
1F8300	Don't Use	-	-
1F8301 - 1F837F	Next series available		

Tag	Name	Format	Length of TLV Value (in Bytes)
CFFFFF05	Optional Data Record Tags (MSD / Magstripe / Non-EMV)	b	Variable

Appendix A.3: Proprietary TLV Tags used by Poynt (Constructed Tags)

A list of proprietary TLV tags that Poynt has used to define constructed data items that do not have Tags in the standard Contact and Contactless EMV specifications or in the card association specific contactless specifications is given in the following table.

Note: Proprietary TLV Tags of the form 3F80xx should not be used (other than those that have already been defined. Instead, Tags of the form 3F81xx should be used.

Tag	Name	Format	Length of TLV Value (in Bytes)	Usage
3F8000	Virtual Dataset Data Items for Transaction Type 00 (Purchase)	b	Variable	Set AID Configuration (MasterCard)
3F8001	Virtual Dataset Data Items for Transaction Type 01 (Cash Advance)	b	Variable	Set AID Configuration (MasterCard)
3F8002	Virtual Dataset Data Items for Transaction Type 09 (Purchase with Cashback)	b	Variable	Set AID Configuration (MasterCard)
3F8003	Virtual Dataset Data Items for Transaction Type 20 (Refund)	b	Variable	Set AID Configuration (MasterCard)
3F8005	DRL Set	b	Variable	Set AID Configuration (Visa)
3F8006	Virtual Dataset Data Items for Transaction Type 21 (Cash Deposit)	b	Variable	Set AID Configuration (Mastercard)
3F8007	Virtual Dataset Data Items for Transaction Type 88 (Invalid TT)	b	Variable	Set AID Configuration (Mastercard). This is for test purposes only.
3F8008	Virtual Dataset Data Items for Transaction Type 12 (Manual Cash)	b	Variable	Set AID Configuration (Mastercard)
3F8009	Virtual Dataset Data Items for Transaction Type 17 (Cash Disbursement)	b	Variable	Set AID Configuration (Mastercard)
3F800A-3F80FF	Don't Use	-	-	Do not use any more Tags in this range since the Tag format is not valid. Use the range 3F81xx.
3F8100	Don't Use	-	-	This is not a valid tag as per BER TLV Rules.
3F8104	Application Item	b	Variable (Max 51)	
3F8105	Acquirer Item	b	Variable	
3F8106	Acquirer Data for Non-Bancomat MSR Tracks	b	Variable	
3F8107	MSR Single Acquirer Data	b	Variable	

Tag	Name	Format	Length of TLV Value (in Bytes)	Usage
3F8108	Acquirer Data for Bancomat MSR Track	b	Variable	
3F8109	Unknown Proprietary Tag List (Mastercard)	b	Variable	Set AID Configuration (Mastercard)

Appendix A.4: PIN Entry UI Configuration Behaviors

There is no standard for how a PIN Entry UI should behave. For example, on some devices the Cancel button is used for PIN Bypass while in others the Enter Button is used for PIN Bypass. Similarly, there is no standard way in which a device should behave if it times out during PIN Entry.

Some customers have very specific requirements for PIN Entry UI behavior in terms of which button means what.

In order to support these different requirements, the PIN Entry UI Config (Tag 1F8171) can be used to define different behaviors for the PIN Entry UI components and events.

The PIN Entry UI Behaviors supported are described in detail in the following sub-sections.

A.4.1 Behavior 1 – PIN Bypass on Cancel

- Enter Button is pressed with No PIN
  - Nothing happens - the button press is ignored.
- Cancel Button is pressed
  - If PIN Bypass is supported: Cancel results in *PIN Bypass* and transaction continues.
  - If PIN Bypass is not supported: Cancel results in Transaction being Cancelled (Terminated).
- PIN Entry Timeout occurs
  - PIN Entry Timeout results in *PIN Pad not Working* and transaction continues.
- Terminal may Cancel Transaction during PIN Entry

A.4.2 Behavior 2 – PIN Bypass on Enter without PIN

- Enter Button is pressed with No PIN
  - If PIN Bypass is supported: Enter with No PIN results in PIN Bypass and transaction continues.
  - If PIN Bypass is not supported: Enter with No PIN is ignored i.e. no action is taken on it.
- Cancel Button is pressed
  - Cancels (Terminates) the transaction regardless of whether PIN Bypass is supported or not.
- PIN Entry Timeout occurs
  - Cancels (Terminates) the transaction regardless of whether PIN Bypass is supported or not.
- Terminal may Cancel Transaction during PIN Entry