

# Heartland

*A Global Payments Company*

---

## Heartland Payment Application v5.0.1

### Functional Specification

Version 1.0

May 2020



## Table of Contents

1. Document Overview	21
1.1. Purpose	21
1.2. Audience	21
2. Heartland Payment Application Overview	21
2.2. Supported Hardware	21
2.3. Supported Industries	21
3. Heartland Payment Application	22
3.1. Overview	22
3.2. Heartland Payment Application States	22
3.2.1. Boot State	22
3.2.2. Lane Closed State	23
3.2.3. Lane Open State	23
3.3. Heartland Payment Application Listener	23
3.3.1. Overview	23
3.3.2. Listener Type	24
3.3.2.1. Serial	24
3.3.2.2. TCP	24
3.3.2.3. Listener Type Settings	24
3.3.3. Listener Protocol	25
3.3.3.1. Serial	25
3.3.3.2. TCP	25
3.3.4. Listener Message Format	26
3.3.4.1. Serial	26
3.3.4.2. TCP	26
4. Transaction Processing	27
4.1. Overview	27
4.2. Connectivity	27
4.3. Heartland Portico Gateway	28
4.3.1. Test Info	28
4.3.2. Production Info	28

4.3.3. Messaging	28
4.3.4. Transactions Supported	28
4.4. Regular Sale, Return and Void	29
4.5. Partial Approvals	30
4.5.1. Partial Approval Prompts	30
4.5.1.1. Partial approval where cashback is not requested	30
4.5.1.2. Partial approval where cashback is not approved and money is owed	31
4.5.1.3. Partial approval where cashback is not approved and money is not owed	31
4.5.1.4. Partial approval where cashback is partially approved and money is not owed	32
4.6. Piggyback transactions	33
4.6.1. Reversals	33
4.6.1.1. Provisional Reversal	34
4.6.2. EMV Chip Card Declines	34
4.6.3. Signature uploads	34
4.6.4. SAF Transactions	34
4.7. SAF Transactions	35
4.7.1. SAF Modes	35
4.7.2. SAF Amount Limit	35
4.7.3. SAF Count Limit	35
4.7.4. SAF Transaction States	36
4.7.5. SAF Eligible Transactions	36
4.7.6. SAF for Credit Auth/Additional Auth/Credit Auth Complete	37
4.7.6.1. SAF Logic for Credit Auth	37
4.7.6.2. SAF Logic for Credit Additional Auth	37
4.7.6.3. SAF Logic for Credit Auth Complete	37
4.7.7. EMV Chip Card Declines After Communications Failure	37
4.7.8. EMV and Voice Auth Offline Approval Communication Failures	38
4.7.9. Credit Adjustment and Void Support for SAF Transactions	38
4.7.10. SAF Reports	39
4.7.11. SAF Retries	39
4.8. Subsequent Transactions	40

4.9. Bar Tab Processing Overview	41
4.9.1. CreditIncrementalAuth and CreditAdditionalAuth Differences	42
4.10. Reboot Recommendation	43
4.11. Contactless Transaction Support	43
5. API Message Definition	44
5.1. XML Syntax	44
5.1.1. Overview	44
5.1.2. Rules	44
5.2. Admin Commands	45
5.2.1. CloseBatch Command	45
5.2.2. Download Command	45
5.2.2.1. Request Schema	46
5.2.2.2. Request Example	46
5.2.2.3. Response Schema	47
5.2.2.4. Response Example	47
5.2.3. EOD Command	48
5.2.3.1. Initiation	48
5.2.3.2. Offline Transaction Processing	48
5.2.3.3. Batch Close Processing	49
5.2.3.4. Request Schema	49
5.2.3.5. Request Example	49
5.2.3.6. Response Schema	49
5.2.3.7. Response Example	50
5.2.3.8. Initiation	52
5.2.3.9. Offline Transaction Processing	52
5.2.3.10. Batch Close Processing	52
5.2.3.11. Request Schema	53
5.2.3.12. Request Example	53
5.2.3.13. Response Schema	53
5.2.3.14. Response Example	54
5.2.4. GetAppInfoReport Command	55

5.2.4.1. Request Schema	55
5.2.4.2. Request Example	56
5.2.4.3. Response Schema	56
5.2.4.4. Record Data	57
5.2.4.5. Response Example	59
5.2.5. GetBatchReport Command	61
5.2.5.1. Request Schema	61
5.2.5.2. Request Example	61
5.2.5.3. Summary Response	61
5.2.5.3.1. Response Schema	62
5.2.5.3.2. Record Data	63
5.2.5.3.3. Response Example	64
5.2.5.4. Detail Response	65
5.2.5.4.1. Response Schema	65
5.2.5.4.2. Record Data	66
5.2.5.4.3. Response Example	68
5.2.6. GetEMVParameterReport Command	69
5.2.6.1. Request Schema	69
5.2.6.2. Request Example	70
5.2.6.3. Response Schema	70
5.2.6.4. Record Data	71
5.2.6.5. Response Example	74
5.2.7. GetLastEODReport Command	75
5.2.7.1. Request Schema	75
5.2.7.2. Request Example	75
5.2.7.3. Response Schema	76
5.2.7.4. Response Example	77
5.2.8. GetLastResponse Command	78
5.2.8.1. Request Schema	78
5.2.8.2. Request Example	78
5.2.8.3. Response Schema	78

5.2.8.4. Response Example	79
5.2.9. GetParameterReport Command	80
5.2.9.1. Request Schema	80
5.2.9.2. Request Example	81
5.2.9.3. Response Schema	81
5.2.9.4. Record Data	82
5.2.10. GetSAFReport Command	90
5.2.10.1. Request Schema	91
5.2.10.2. Request Example	91
5.2.10.3. Response Schema	91
5.2.10.4. Record Data	92
5.2.10.5. Response Example	94
5.2.11. LaneClose Command	95
5.2.11.1. Request schema	95
5.2.11.2. Request Example	95
5.2.11.3. Response Schema	95
5.2.11.4. Response Example	96
5.2.12. LaneOpen Command	96
5.2.12.1. Request Schema	96
5.2.12.2. Request Example	97
5.2.12.3. Response Schema	97
5.2.12.4. Response Example	98
5.2.13. ManagerMenu Command	98
5.2.13.1. Request Schema	98
5.2.13.2. Request Example	99
5.2.13.3. Response Schema	99
5.2.13.4. Response Example	99
5.2.14. Reboot Command	100
5.2.14.1. Request Schema	100
5.2.14.2. Request Example	100
5.2.14.3. Response Schema	100

5.2.14.4. Response Example	101
5.2.15. Reset Command	101
5.2.15.1. Request Schema	102
5.2.15.2. Request Example	102
5.2.15.3. Response Schema	103
5.2.15.4. Response Example	103
5.2.16. SendFile Command	104
5.2.16.1. Supported Files	104
5.2.16.2. Request Schema	105
5.2.16.3. Response Schema	105
5.2.16.4. Initial FileName Request Example	106
5.2.16.5. Initial FileName Response Example	106
5.2.16.6. Subsequent FileData Request Examples	106
5.2.16.7. FileData Response Example	107
5.2.16.8. Error Response Example	108
5.2.17. SendSAF Command	108
5.2.17.1. Request Schema	108
5.2.17.2. Request Example	109
5.2.17.3. Response Schema	109
5.2.17.4. Record Data	110
5.2.17.5. Response Example	111
5.2.18. SetClock Command	112
5.2.18.1. Request Schema	112
5.2.18.2. Request Example	112
5.2.18.3. Response Schema	112
5.2.18.4. Response Example	113
5.2.19. SetParameter Command	114
5.2.19.1. Request Schema	114
5.2.19.2. Request Example	114
5.2.19.3. Response Schema	115
5.2.19.4. Response Example	115

5.3. Transaction Commands	116
5.3.1. AddValue Command	116
5.3.1.1. Request Schema	116
5.3.1.2. Request Example	117
5.3.1.3. Response Schema	117
5.3.1.4. Response Example	119
5.3.1.5. Gift Card Whitelist Add Value	119
5.3.1.5.1. Gift Card Add Value Request Schema	119
5.3.1.5.1.1. Request Example	120
5.3.1.5.1.2. Response Example	120
5.3.2. BalanceInquiry Command	120
5.3.2.1. Request Schema	120
5.3.2.2. Request Example	121
5.3.2.3. Response Schema	121
5.3.2.4. Response Example	122
5.3.3. CardVerify Command	123
5.3.3.1. Request Schema	123
5.3.3.2. Request Example	124
5.3.3.3. Response Schema	124
5.3.3.4. Response Example	126
5.3.4. CreditAuth Command	127
5.3.4.1. Request Schema	127
5.3.4.2. Request Example	128
5.3.4.3. Response Schema	128
5.3.4.4. Response Example	130
5.3.5. CreditAdditionalAuth Command	130
5.3.5.1. Request Schema	131
5.3.5.2. Request Example	131
5.3.5.3. Response Schema	131
5.3.5.4. Response Example	132
5.3.6. CreditAuthComplete Command	132



5.3.6.1. Request Schema	133
5.3.6.2. Request Example	133
5.3.6.3. Response Schema	133
5.3.6.4. Response Example	134
5.3.7. GetCardData Command	135
5.3.7.1. Request Schema	135
5.3.7.2. Request Example	136
5.3.7.3. Response Schema	136
5.3.7.4. Response Example	137
5.3.8. LineItem Command	137
5.3.8.1. Line Item Display	137
5.3.8.2. Subsequent Processing	138
5.3.8.3. Request Schema	138
5.3.8.4. Request Example	139
5.3.8.5. Response Schema	139
5.3.8.6. Response Example	140
5.3.9. Notification Message	140
5.3.9.1. Notification Enablement	140
5.3.9.2. <Status> Element	140
5.3.9.3. Request Schema	141
5.3.9.4. Response Schema for CARD PRESENTED	141
5.3.9.5. Response Example for CARD PRESENTED	142
5.3.9.6. Notification Messages for Unsupported Status Element Values	142
5.3.10. Refund Command	143
5.3.10.1. SAF Processing	143
5.3.10.2. Processing Errors	144
5.3.10.3. Refund Flow	144
5.3.10.4. Request Schema	144
5.3.10.5. Request Example	145
5.3.10.6. Response Schema	145
5.3.10.7. Response Example	147

5.3.11. Reset Command	147
5.3.11.1. Request Schema	148
5.3.11.2. Request Example	148
5.3.11.3. Response Schema	149
5.3.11.4. Response Example	149
5.3.11.5. Card Acquisition Cancellation During StartCard	150
5.3.12. Sale Command	150
5.3.12.1. Card Category Prompt	150
5.3.12.2. Card Acquisition Prompt	150
5.3.12.3. Application Selection Prompt	151
5.3.12.4. PIN Prompt	151
5.3.12.5. Subsequent Processing	152
5.3.12.6. Request Schema	152
5.3.12.7. Request Example	153
5.3.12.8. Response Schema	153
5.3.12.9. Response Example	156
5.3.12.10. Gift Card Whitelist Sale	157
5.3.12.10.1. Request Example	157
5.3.12.10.2. Response Example	158
5.3.12.10.3. Whitelist Gift Card Sale Response	158
5.3.12.10.4. Display Message Request	159
5.3.12.10.5. Display Message Response	159
5.3.13. StartCard Command	159
5.3.13.1. Request Schema	160
5.3.13.2. Request Example	160
5.3.13.3. Response Schema	160
5.3.13.4. Response Example	161
5.3.14. TipAdjust Command	161
5.3.14.1. Request Schema	161
5.3.14.2. Request Example	162
5.3.14.3. Response Schema	162

5.3.14.4. Response Example	163
5.3.15. TransactionAdjust Command	163
5.3.15.1. SAF Processing	164
5.3.15.2. Processing Errors	164
5.3.15.3. TransactionAdjust Flow	165
5.3.15.4. Request Schema	165
5.3.15.5. Request Example	165
5.3.15.6. Response Schema	166
5.3.15.7. Response Example	167
5.3.16. VoiceAuth Command	167
5.3.16.1. Request Schema	168
5.3.16.2. Request Example	168
5.3.16.3. Response Schema	168
5.3.16.4. Response Example	170
5.3.17. Void Command	171
5.3.17.1. SAF Processing	171
5.3.17.2. Processing Errors	171
5.3.17.3. Void Flow	172
5.3.17.4. Request Schema	172
5.3.17.5. Request Example	173
5.3.17.6. Response Schema	173
5.3.17.7. Response Example	174
5.4. XML Elements	175
5.4.1. <AdditionalTipAmount>	175
5.4.2. <ApplicationId>	175
5.4.3. <ApprovalCode>	175
5.4.4. <Attachment>	175
5.4.5. <AttachmentData>	176
5.4.6. <AuthorizedAmount>	176
5.4.7. <AvailableBalance>	176
5.4.8. <AVS>	176

5.4.9. <AVSResultText>	177
5.4.10. <BalanceAmount>	177
5.4.11. <BalanceDueAmount>	177
5.4.12. <BaseAmount>	177
5.4.13. <BatchClose>	177
5.4.14. <ButtonText>	178
5.4.15. <CardAcquisition>	178
5.4.16. <CardGroup>	178
5.4.17. <CardholderName>	179
5.4.18. <CardType>	179
5.4.19. <CashbackAmount>	179
5.4.20. <ChoiceSelected>	179
5.4.21. <ClearPAN>	179
5.4.22. <ConfirmAmount>	180
5.4.23. <CVV>	180
5.4.24. <CVVResultText>	181
5.4.25. <DataEntered>	181
5.4.26. <DateTime>	181
5.4.27. <DeviceId>	181
5.4.28. <DownloadTime>	181
5.4.29. <DownloadType>	182
5.4.30. <EBTAmount>	182
5.4.31. <EBTType>	182
5.4.32. <ECRId>	182
5.4.33. <EditBoxFormat>	182
5.4.34. <EMV_AID>	183
5.4.35. <EMV_ApplicationName>	183
5.4.36. <EMV_Cryptogram>	183
5.4.37. <EMV_CryptogramType>	184
5.4.38. <EMV_TSI>	184
5.4.39. <EMV_TVR>	184

5.4.40. <EMVOfflineDecline>	184
5.4.41. <EMVPDL>	184
5.4.42. <EODEndTime>	185
5.4.43. <EODStartTime>	185
5.4.44. <Field>	185
5.4.45. <FieldCount>	185
5.4.46. <FileName>	185
5.4.47. <FileData>	186
5.4.48. <FileSize>	186
5.4.49. <FormText>	186
5.4.50. <GatewayRspCode>	186
5.4.51. <GatewayRspMsg>	186
5.4.52. <HeartBeat>	187
5.4.53. <HUDSPORT>	187
5.4.54. <HUDSURL>	187
5.4.55. <InvoiceNbr>	187
5.4.56. <Key>	187
5.4.57. <LastResponse>	188
5.4.58. <LeftButtonText>	188
5.4.59. <LineItemRunningTextLeft>	188
5.4.60. <LineItemRunningTextRight>	188
5.4.61. <LineItemTextLeft>	188
5.4.62. <LineItemTextRight>	189
5.4.63. <MaskedPAN>	189
5.4.64. <MaxDataSize>	189
5.4.65. <MultipleMessage>	189
5.4.66. <OrigTransactionId>	190
5.4.67. <PartialApproval>	190
5.4.68. <PinVerified>	190
5.4.69. <QPSQualified>	190
5.4.70. <Record>	191

5.4.71. <ReferenceNumber>	191
5.4.72. <Request>	191
5.4.73. <RequestId>	192
5.4.74. <Response>	193
5.4.75. <ResponseCode>	194
5.4.76. <ResponseId>	194
5.4.77. <ResponseText>	194
5.4.78. <Result>	195
5.4.79. <ResultText>	198
5.4.80. <Reversal>	199
5.4.81. <RightButtonText>	199
5.4.82. <SendSAF>	199
5.4.83. <ServerLabel>	199
5.4.84. <SignatureLine>	199
5.4.85. <SignaturePrompt>	200
5.4.86. <SIP>	200
5.4.87. <SIPId>	200
5.4.88. <Status>	200
5.4.89. <StoreAndForward>	201
5.4.90. <TableCategory>	201
5.4.91. <TaxAmount>	201
5.4.92. <TerminalId>	201
5.4.93. <Time>	202
5.4.94. <TipAdjustAllowed>	202
5.4.95. <TipAmount>	202
5.4.96. <TokenRequest>	202
5.4.97. <TokenRspCode>	202
5.4.98. <TokenRspMsg>	203
5.4.99. <TokenValue>	203
5.4.100. <TotalAmount>	203
5.4.101. <TrackData>	203

5.4.102. <TrackNumber>	204
5.4.103. <TransactionCertificate>	204
5.4.104. <TransactionId>	204
5.4.105. <TransactionIdType>	205
5.4.106. <TransactionTime>	205
5.4.107. <Value>	205
5.4.108. <Version>	205
5.5. Result and Response Codes	206
5.5.1. HPA Error	206
5.5.2. Offline Decline	207
5.5.3. Gateway Error	207
5.5.4. Store-and-Forward Response	207
5.5.5. Host Response	208
5.5.6. HPA Result Codes	208
5.5.7. Offline Response Codes	214
5.5.8. Portico Gateway Response Codes	214
5.5.9. Exchange Host Response Codes	217
5.5.10. Chockstone Host Response Codes	220
5.6. SIP Response to POS Communication Failure	221
5.6.1. Request Example	222
5.6.2. Response Example	222
6. Heartland Payment Application Features	224
6.1. Quick Chip	224
6.1.1. Predetermined Amount	224
6.1.2. Internal Processing	225
6.2. Card Type Determination	226
6.2.1. <CardGroup> Element	226
6.2.2. CRDCATPRMPT = 0 (Disabled)	227
6.2.3. CRDCATPRMPT = 1 (Enabled)	228
6.2.4. CRDCATPRMPT = 2 (Conditional)	228
6.3. Tip Processing	229

6.3.1. Tip Enablement	229
6.3.2. Tip Prompting	230
6.3.2.1. Add Tip Prompt	231
6.3.2.2. Add Additional Tip Prompt	231
6.3.2.3. Basic Tip Prompt	231
6.3.2.4. Tip Assist Prompt	232
6.3.2.5. Split Tip Prompt	232
6.3.3. <TipAmount> Element	234
6.3.4. <AdditionalTipAmount> Element	234
6.3.5. <TipAdjustAllowed> Element	234
6.3.6. TipAdjust Command	235
6.4. Cashback Processing	235
6.4.1. Cashback Enablement	235
6.4.2. Cashback Prompting	236
6.4.2.1. Basic Cashback Prompt	236
6.4.2.2. Cashback Assist Prompt	237
6.4.3. Cashback Limit	237
6.4.4. <CashbackAmount> Element	238
6.5. Signature Capture	239
6.5.1. Signature Capture on SIP	239
6.5.2. Signature Data to Portico	239
6.5.3. Signature Data to POS	239
6.6. Cancel Key Configuration	240
6.7. Software Updates	241
6.7.1. Heartbeat Disablement	241
6.7.2. Download Command	241
6.8. Power Management	242
6.8.1. Sleep Mode	242
6.8.2. Battery Level Indicator	243
6.8.3. Battery Level Warning	243
6.9. Whitelist Processing	244



6.10. Batch Retrieval	244
6.11. Ping Remote URL	245
7. User Interface	247
7.1. Common UI behavior	247
7.2. Graphical Payment Flow	248
7.2.1. Overview	248
7.2.2. Idle Logo	248
7.2.3. Promotional Images	248
7.2.4. Banner	249
Banner Top Layout (UILAYOUT = 1)	249
Banner Left Layout (UILAYOUT = 2)	249
7.2.5. Status Screen	251
Banner Top Layout	251
Banner Left Layout	251
7.2.6. Choice Screen	252
The choice screen template contains text and buttons. This screen is used to present a choice to the consumer so the consumer can select the choice (button). For example, on a card type selection, Yes/No screen, etc.	
7.2.7. Edit Screen	252
7.3. GUI Customization	253
7.3.1. Color and Image Customization	253
7.3.1.1. BackgroundImage	253
7.3.1.2. PromptTextColor	253
7.3.1.3. ButtonTextColor	254
7.3.1.4. ButtonBkgColor	254
7.3.2. Promotional Images	255
7.3.2.1. PromolImageDisplay	255
7.3.2.2. PromoDisplayTime	255
7.3.2.3. PromolImage1 to PromolImage10	256
7.4. Display Rules	256
7.4.1. Rules for displaying prompt lines	256
7.5. SetKeys	257
7.5.1. Application settings	257

7.6. Custom Forms	257
7.6.1. Status Form	258
7.6.1.1. Request Schema	259
7.6.1.2. Request Example	259
7.6.1.3. Response Schema	260
7.6.1.4. Response Example	260
7.6.2. Choice Form	260
7.6.2.1. Request Schema	262
7.6.2.2. Request Example	262
7.6.2.3. Response Schema	263
7.6.2.4. Response Example	263
7.6.3. Edit Form	264
7.6.3.1. Request Schema	264
7.6.3.2. <FormText>	265
7.6.3.3. <EditBoxFormat>	265
7.6.3.4. Request Example	266
7.6.3.5. Response Schema	266
7.6.3.6. Response Example	267
7.6.4. Signature Form	267
7.6.4.1. Request Schema	268
7.6.4.2. Request Example	268
7.6.4.3. Response Schema	268
7.6.4.4. Response	269
7.7. Error Messages	269
7.7.1. Transaction Canceled	269
7.7.2. HPA Error	269
7.7.3. User Error	270
7.8. Quick Access Screen	270
8. Parameters	272
8.1. Overview	272
8.2. Communication Parameters	273

8.3. Display/Prompt Parameters	277
8.4. Download Parameters	281
8.5. Merchant Parameters	283
8.6. Network Parameters	287
8.7. Password Parameters	290
8.8. Transaction Parameters	291
8.9. Serial Parameters	298
8.10. Credential Sharing Between Downloader and HPA	299
9. Appendices	301
9.1. Glossary	301
9.2. BIN Table	303
9.2.1. Overview	303
9.2.2. Sample BIN Table	305
9.2.3. BIN Range Setup	307
9.2.4. BIN Range Validation	308
9.2.5. Security Code	308
9.2.6. Tip Discount Rate	308
9.2.7. B.7 QPS Limit	309
9.2.8. Expiration Date Check	309
9.2.9. AVS	310
9.2.10. Manual Entry Allowed	310
9.2.11. Luhn Check	310
9.3. EMV PDL Setup	310
9.4. Portico Setup	311
9.5. HUDS Setup	311
9.6. HPA SDK	311
9.6.1. Overview	311
9.7. HPA Installation	312
9.7.1. Installation Overview	312
9.7.2. Set the terminal date and time	312
9.7.3. Clean the Terminal	313

9.7.4. Baseline Installation Overview	313
9.7.5. Installing Baseline/HeartLoader Using LLT	313
9.7.5.1. Baseline with HeartLoader Installation on Lane/3000 and Lane/5000	313
9.7.6. Field Upgrade By Merchants Running RBA	314
9.7.6.1. Prerequisites	314
9.7.6.2. Point Of Sale Development for Upgrading RBA Terminals	314
9.7.7. Loading Test DUKPT/EMV keys	315
9.7.7.1. Overview	315
9.7.7.2. Get the SIP device ready for key injection	315
9.7.7.3. Load keys from PC	315
9.8. HeartLoader	316
9.8.1. Overview	316
9.8.2. Boot	316
9.8.3. Idle Screen	317
9.8.4. Initializing Screen	317
9.8.5. Update Failed Screen	317
9.8.6. Error Screen	317
9.8.7. Login Screen	318
9.8.8. Configuration	318
9.8.8.1. SETTINGS.TXT	318
9.8.8.2. Default Settings	319
9.8.8.3. STATICIPS.TXT	320
9.8.8.4. Initiating HPA Download	320
9.8.8.5. StartDownload	320
9.8.8.5.1. Request	321
9.8.8.5.2. H.8.5.2 Response	321
9.8.8.6. Manual Download	321
9.8.8.7. After Download	322
9.8.8.8. HeartLoader Integration Notes	322
9.9. Heartland Universal Download System (HUDS) Environments	322
9.9.1. HUDS Development Environment	322

9.9.2. HUDS Production Environment	322
9.9.3. Application ID and Terminal ID	323
9.9.3.1. Application IDs for HeartLoader and HPA	323
9.9.3.2. HUDS HeartLoader TIDs & AppIDs	323
9.10. HeartPOS	324
9.10.1. Overview	324
9.10.2. Environment	324
9.10.3. Build/Run HeartPOS	324
9.10.4. Configuration	324
9.10.5. HeartPOS UI	326
9.10.6. HeartPOS Usage	326
9.10.7. Transactions Supported	328
9.11. HPA ZIP File List and Description	329
9.12. HeartPOS SDK	329
9.12.1. Overview	329
9.12.2. HPA Class	329
9.12.2.1. Connecting to SIP device	330
9.12.2.2. Send command/message to SIP device	330
9.12.2.3. Receive command/message from SIP device	330
9.12.2.4. Disconnect from SIP device	330
9.12.3. HeartPOS Class	331
9.12.3.1. XML Pack	331
9.12.3.2. XML Unpack APIs	331

# 1. Document Overview

## 1.1. Purpose

This document describes the Heartland Payment Application (HPA) 5.X semi-integrated payment application. HPA is based on the widely deployed Spectrum application. For complete features of Spectrum, please refer to the Spectrum 5.X Functional Specification document which describes the application in a stand-alone mode along with a detailed description of each feature.

## 1.2. Audience

The intended audience of this document includes software developers, business analysts, QA personnel, and other personnel at both internal and external vendors who chose to integrate their POS (or ECR) system with a Semi-Integrated Peripheral (SIP) device running HPA 5.X.

# 2. Heartland Payment Application Overview

## 2.2. Supported Hardware

HPA runs on the following SIP devices:

Device	Description
Ingenico Lane/3000	This is a non-touchscreen GUI device display.
Ingenico Lane/5000	This is a touchscreen GUI device capable of signature capture.

## 2.3. Supported Industries

HPA supports the following industries:

- Retail
- Restaurant

## 3. Heartland Payment Application

### 3.1. Overview

In SIP mode, the application is driven by a POS (aka ECR) system. When a terminal is running the application in SIP mode the device is referred to as the “SIP device”.

The SIP device is connected to a POS system (typically but not necessarily Windows based) by an Ethernet, Wi-Fi, USB, or RS-232 connection.

The POS is responsible for ringing up items; when the time comes for payment, it sends a command to the SIP device running HPA to process a payment.

HPA listens for commands from the POS. When a command is received, it processes the command, typically a payment request transaction. HPA processes the entire transaction including card acquisition and additional prompting if required, and authorizes it through Heartland via TCP/IP. The result of the transaction and receipt data is sent back to the POS so that the POS can print a receipt and store the result for reporting.

HPA insulates the POS from cardholder data so that the POS is out-of-scope for PCI and EMV card brand certification.

HPA is EMV certified and is presented as a black box to POS vendors to support EMV via simple POS integration.

### 3.2. Heartland Payment Application States

#### 3.2.1. Boot State

In the boot state, it performs the following checks in this order:

- Initialization: at power-up HPA goes through an initialization sequence in which it initializes the application.
- EMV Initialization:
  - If the SIP device contains downloaded EMV parameters, it will continue using those parameters.
  - If the SIP device does not contain downloaded EMV parameters, it will use default EMV parameters instead, and it will download EMV parameters when EOD is processed.

- If the SIP device does not contain downloaded EMV parameters, and default EMV parameters are not available, it will download the EMV parameters.
- If the SIP device does not contain downloaded EMV parameters, default EMV parameters are not available, and the EMV parameter download fails, EMV will be disabled until EMV parameters are downloaded when EOD is processed.
- After performing the above checks HPA goes to the Lane Closed state.

### 3.2.2. Lane Closed State

HPA displays a “Lane Closed” screen. In this state, it is waiting for admin commands from the ECR to process. Examples of admin commands include Close Batch, Get Batch Report, Send Store and Forwards, Get Store and Forward Report, Get Application Information Report, Get Parameter Report, Get EMV PDL Report (EMV Parameters), and Re-boot.

The default “LANE CLOSED” text that appears at the bottom of this screen can be modified via the **LCLOSETEXT** application parameter.

### 3.2.3. Lane Open State

HPA displays a “LANE OPEN” screen. In this state, it is waiting for transaction commands to process from the ECR. Examples of transactions include Sale, Refund, Void, etc.

The default “LANE OPEN” text that appears at the bottom of this screen can be modified via the **LOPENTEXT** application parameter.

## 3.3. Heartland Payment Application Listener

### 3.3.1. Overview

- HPA has a listener waiting for commands from POS to process.
- The POS sends a command request and HPA responds with a command response.
- The typical usage is POS sends one command request and HPA sends a command response back after processing the request.
- HPA can take a few seconds or sometimes a minute (depending on the application timeout settings) to respond depending on the command to process. The POS needs to wait for the response.
- If there is no response from HPA prior to timing out, the POS can send a reset command.



- Sometimes, HPA can send multiple command responses to a single command request. For example, a report.
- Sometimes, POS would need to send multiple command requests for a single action. For example, sending a file. In this case, each command request will get a command response from HPA.
- Sometimes, HPA can send a progress response to indicate the progress of the command request that HPA is working on such as a card inserted or swiped progress response.

### 3.3.2. Listener Type

#### 3.3.2.1. Serial

When configured for serial, HPA sets up a Serial Listener using the Listener Type Serial settings.

- The POS is required to open its serial port and configure the serial settings to the same values as in Listener Type serial settings to establish a serial connection between the POS and HPA.
- The POS can keep this serial connection open as long as it wants.

#### 3.3.2.2. TCP

HPA sets up a TCP Socket Listener using the Listener Type settings. HPA keeps the listener socket connection open until the POS closes it or if there is a system error or a reboot.

At the physical layer the TCP communication can be carried over either Ethernet or Wi-Fi.

#### 3.3.2.3. Listener Type Settings

The Listener Type (Serial vs. TCP) and their settings are set by the following in this order.

- Manually during HPA bootup – this will change the HPA Listener parameters locally
- If not manually set, uses HPA Listener parameters from HUDS, if any
- If no parameters, use Settings.txt if present
- If POSLINKTYPE or POSLINKSET are empty, use defaults – POSLINKTYPE=2 (TCP); POSLINKSET=12345
- If network parameters are not set, use defaults – NETDHCP=1
- The parameter IPCONNTYPE determines if the TCP communication goes over Ethernet or over Wi-Fi. If this parameter is set to 1, then the Ethernet physical interface is used for TCP communication. If it is set to 2 then Wi-Fi interface is used for TCP communication.

### 3.3.3. Listener Protocol

#### 3.3.3.1. Serial

HPA uses the standard ACK/NAK protocol to verify that the message is sent correctly without any parity errors. Note that the SIP device responds with an explicit ACK to the command from the POS rather than using an implied ACK (i.e. sending the command response as implicit ACK) since for some commands there may be a time delay before the SIP response is sent back to the POS.

The POS response is also formatted as:

<STX> ... Message... <ETX>[LRC].

If the POS detects a LRC error then it should respond with a NAK which will result in the SIP device resending the response.

The normal flow is shown below.

POS	SIP Device / HPA
Request Command →	
	← ACK
	← Initial Response Packet
ACK →	
	← Other Response Packet(s)
ACK →	
	← Final Response Packet
ACK →	

#### 3.3.3.2. TCP

TCP protocol handles message integrity and delivery, hence the ACK/NAK protocol is not used for TCP communication between the POS and the SIP device.

### 3.3.4. Listener Message Format

#### 3.3.4.1. Serial

The message format is:

<STX>...Message...<ETX>[LRC]

STX and ETX are standard control characters, 0x02 and 0x03, respectively.

The LRC is a standard Longitudinal Redundancy Check computed by the contents of the message starting with the first byte after the <STX> and including the ETX. If the LRC is not correct the SIP device will respond with a NAK (0x15) character.

#### 3.3.4.2. TCP

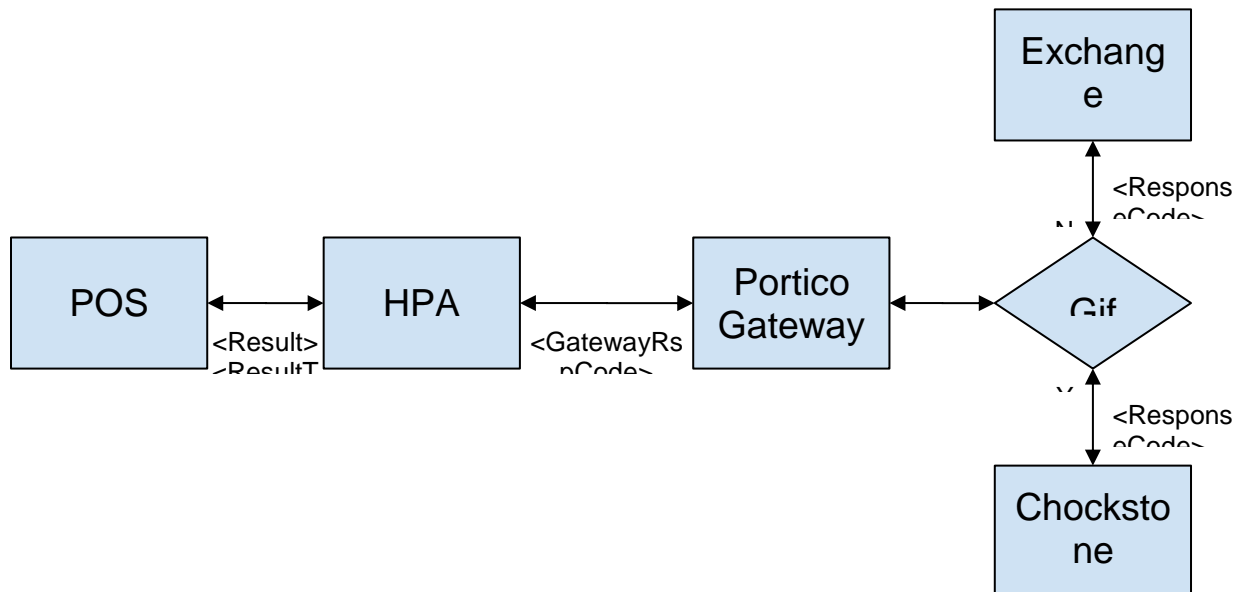
The TCP message does not wrap the message with <STX> ... <ETX>[LRC] characters.

The TCP message has a two byte message header prepended to the start of the message. The two byte message header is the length of the message not including the two byte header, and is sent with the most significant byte first.

## 4. Transaction Processing

### 4.1. Overview

HPA processes transactions using the Heartland Portico Gateway. Credit, Debit, and EBT transactions are routed from the Portico gateway to the Exchange host for authorization. Heartland Gift card transactions are routed to the Chockstone host for authorization.



### 4.2. Connectivity

HPA uses only IP connectivity to connect to the host.

HPA supports configurable Primary and Secondary URLs for TCP/IP communication with the host and toggles automatically between the Primary and Secondary URLs to maintain TCP/IP communication. Both primary and secondary URLs can be verified using the Parameter Report (GetParameterReport) or Admin Menu.

Host URL switching logic works as follows:

- HPA defaults to the Primary URL as the preferred URL.
- HPA tries to connect to both URLs in an alternating fashion, starting with the preferred URL, e.g. Primary > Secondary > Primary > Secondary, or Secondary > Primary > Secondary > Primary depending on which one is preferred at the time, and the retry counter of both URLs.

- If HPA is able to connect to a URL, send the request, and receive a response that is not a system error, then it will save that as the preferred URL to start with for the next transaction.
- If HPA is able to connect to a URL, but cannot send the request, timeout waiting for a response, or receive a response that is a system error, then it will save the other URL as the preferred URL to start with for the next transaction.
- If HPA is unable to connect to either URL, or EOD is successfully performed, it will revert back to the Primary URL being the preferred URL.
- The preferred URL at any given time is shown as the START HOST URL (**STARTURL**) parameter under the Communication category in the Parameter Report and Admin Menu. **STARTURL** will be set to one of the following values:
  - 1 = Primary URL (application default)
  - 2 = Secondary URL

## 4.3. Heartland Portico Gateway

### 4.3.1. Test Info

cert.api2-c.heartlandportico.com:443

### 4.3.2. Production Info

api2-c.heartlandportico.com:443

### 4.3.3. Messaging

HPA uses XML messaging to talk to Portico. HPA uses the following Portico messages.

### 4.3.4. Transactions Supported

HPA Transaction	Portico Message
Credit Sale	CreditSale
Credit Refund	CreditReturn
Card Verify	CreditAccountVerify
Credit Auth	CreditAuth
Voice Auth	CreditOfflineSale

Tip Adjust	CreditTxnEdit
Debit Sale	DebitSale
Debit Refund	DebitReturn
EBT Balance Inquiry	EBTBalanceInquiry
EBT CB Sale	EBTCashBackPurchase
EBT CB Refund	Not Applicable
EBT FS Sale	EBTFSPurchase
EBT FS Refund	EBTFSTReturn
Void	CreditVoid, GiftCardVoid, EBTFSTReversal  <b>NOTE:</b> Void is not currently supported for Debit
Reversal	CreditReversal, DebitReversal, GiftCardReversal, EBTFSTReversal
Signature	AddAttachment
EMV Chip Declines	ChipCardDecline
Gift Balance Inquiry	GiftCardBalance
Gift Sale/Redeem	GiftCardSale
Gift Add Value	GiftCardAddValue

## 4.4. Regular Sale, Return and Void

When the POS sends a command, HPA goes through the consumer prompts (if any), builds the request message, sends it to the host, waits for a response from the host (with a timeout), and when the response is received, parses it and sends the response details to the POS in the response elements. HPA sends authorization request to host for POS sent <TotalAmount> for all transactions except EBT food stamp Sale, where it sends EBT eligible amount i.e. <EBTAmount> for authorization.

## 4.5. Partial Approvals

Partial Approvals are supported for the following transactions:

- Credit Sale
- Credit Auth
- Debit Sale
- Gift Card Sale
- EBT CB Sale
- EBT FS Sale

For partial approvals, the SIP device displays prompts indicating that the transaction was only partially approved and prompts the cardholder as to whether they want to continue the transaction or cancel the transaction. If the cardholder cancels the transaction then the SIP device will automatically create a reversal for the partially approved transaction. If the cardholder accepts the transaction then the SIP response to the POS indicates that the transaction was partially approved with the approved amount and balance due.

**NOTE:** Transaction adjustments are not recommended on partially approved transactions, given that additional funds may not be available on the customer's card. For partially approved transactions, HPA will return <TipAdjustAllowed>0</TipAdjustAllowed>.

### 4.5.1. Partial Approval Prompts

If **PartialAuthConfirm** = 1...

#### 4.5.1.1. Partial approval where cashback is not requested

Heartland	Heartland
<b>PARTIALLY APPROVED</b> CREDIT SALE: \$50.00  APPROVED: \$30.00 DUE: \$20.00	<b>PARTIALLY APPROVED</b> CREDIT SALE: \$50.00  APPROVED: \$30.00 DUE: \$20.00 1=ACCEPT 2=DECLINE
<div>ACCEPT</div> <div>DECLINE</div>	

If ACCEPT selected, or **PartialAuthConfirm** = 0...

Heartland	Heartland
<b>PARTIALLY APPROVED</b> CREDIT SALE: \$50.00	<b>PARTIALLY APPROVED</b> CREDIT SALE: \$50.00

<p>APPROVED: \$30.00 DUE: \$20.00</p> <p>ADDITIONAL PAYMENT NEEDED</p>	<p>APPROVED: \$30.00 DUE: \$20.00</p> <p>NEED ANOTHER PAYMENT</p>
--	---

#### 4.5.1.2. Partial approval where cashback is not approved and money is owed

In this example, the base amount was \$30.00 and cashback amount requested was \$20.00.

If **PartialAuthConfirm** = 1 :

Heartland	Heartland
<p><b>PARTIALLY APPROVED</b> DEBIT SALE: \$50.00</p> <p>APPROVED: \$20.00 DUE: \$10.00 (NO CASHBACK)</p>	<p><b>PARTIALLY APPROVED</b> DEBIT SALE: \$50.00</p> <p>APPROVED: \$20.00 DUE: \$10.00 (NO CASH)</p>
<p>ACCEPT</p> <p>DECLINE</p>	<p>1=ACCEPT 2=DECLINE</p>

If ACCEPT selected, or **PartialAuthConfirm** = 0 :

Heartland	Heartland
<p><b>PARTIALLY APPROVED</b> DEBIT SALE: \$50.00</p> <p>APPROVED: \$20.00 DUE: \$10.00 (NO CASHBACK)</p> <p>ADDITIONAL PAYMENT NEEDED</p>	<p><b>PARTIALLY APPROVED</b> DEBIT SALE: \$50.00</p> <p>APPROVED: \$20.00 DUE: \$10.00 (NO CASH)</p> <p>NEED ANOTHER PAYMENT</p>

#### 4.5.1.3. Partial approval where cashback is not approved and money is not owed

In this example, the base amount was \$30.00 and the cashback amount requested was \$20.00.

If **PartialAuthConfirm** = 1 :

Heartland	Heartland
<p><b>PARTIALLY APPROVED</b> DEBIT SALE: \$50.00</p> <p>APPROVED: \$30.00</p>	<p><b>PARTIALLY APPROVED</b> DEBIT SALE: \$50.00</p> <p>APPROVED: \$30.00</p>



NO CASHBACK AVAILABLE		NO CASH AVAILABLE 1=ACCEPT 2=DECLINE
ACCEPT	DECLINE	

If ACCEPT selected, or **PartialAuthConfirm** = 0 :

<b>Heartland</b>  <b>PARTIALLY APPROVED</b> DEBIT SALE: \$50.00  APPROVED: \$30.00 NO CASHBACK AVAILABLE	<b>Heartland</b>  <b>PARTIALLY APPROVED</b> DEBIT SALE: \$50.00  APPROVED: \$30.00 NO CASH AVAILABLE
--	--

#### 4.5.1.4. Partial approval where cashback is partially approved and money is not owed

In this example, the base amount was \$30.00 and the cashback amount requested was \$20.00.

If **PartialAuthConfirm** = 1:

<b>Heartland</b>  <b>PARTIALLY APPROVED</b> DEBIT SALE: \$50.00  APPROVED: \$40.00 CASHBACK: \$10.00	<b>Heartland</b>  <b>PARTIALLY APPROVED</b> DEBIT SALE: \$50.00  APPROVED: \$40.00 CASHBACK: \$10.00 1=ACCEPT 2=DECLINE
<div>ACCEPT</div> <div>DECLINE</div>	

If ACCEPT selected, or **PartialAuthConfirm** = 0 :

<b>Heartland</b>  <b>PARTIALLY APPROVED</b> DEBIT SALE: \$50.00  APPROVED: \$40.00 CASHBACK: \$10.00	<b>Heartland</b>  <b>PARTIALLY APPROVED</b> DEBIT SALE: \$50.00  APPROVED: \$40.00 CASHBACK: \$10.00
--	--

**NOTE:** The SIP device remains on this screen until a new command is received from the POS.

The POS should then initiate a follow up transaction for the balance due amount to complete the sale.

## 4.6. Piggyback transactions

The following transactions are stored in a local transaction file and sent with the next online transaction (i.e. “piggybacked”), sent in the order listed below one by one before sending the current transaction:

- Reversals (CreditReversal, DebitReversal, GiftCardReversal, EBTFSReversal)
- EMV Offline Decline (ChipCardDecline)
- Signature Capture (AddAttachment) – only supported on Lane/5000
- Store And Forward (Credit Sale, Credit Refund, Voice Auth, CreditAuth)

The following processing rules are enforced:

- If a response from the host is not received, it remains in the local transaction file to be sent in the next online transaction.
- Once a response for a pending SAF is received, it is stored in the local transaction file for reporting using the GetSAF command.
- Any piggyback transaction that is uploaded and receives a response from the host is considered successful, regardless of the host response.

### 4.6.1. Reversals

HPA creates a transaction reversal in the following situations:

- When a request is sent, no response is obtained, and the transaction is not eligible for Store and Forward. Before a SAF reversal is sent to Portico, a message is sent to Portico to determine if the transaction already exists.
- When a request is sent and an unknown response or a response that HPA cannot parse is received.
- When a request is sent and there is a power failure before the transaction is completely processed.
- When the transaction is cancelled by the POS at the signature prompt.
- When HPA cannot send an approval response back to POS.

These reversals are stored in a local transaction file to be sent in the next online transaction (piggy backed). This is to reverse the transaction at the host. It is expected that the clerk re-runs the transaction.

Reversals are supported for the following transactions:

- Sale: Credit, Debit, Gift, EBT (Food Stamp and Cash Benefits)
- Refund: Credit, Debit
- Voice Auth
- Credit Auth

#### **4.6.1.1. Provisional Reversal**

Provisional Reversal will get stored, if the transaction was online approved, but HPA is unable to send the response back to the POS. HPA will process the Provisional Reversal according to below scenarios:

- If the POS resends the same <Request>, <RequestId>, and <ECRId> in the next transaction, HPA will discard the Provisional Reversal and return the stored response to the POS.
- If the POS sends a different <Request>, <RequestId>, or <ECRId> in the next transaction, HPA will first process the Provisional Reversal and then process the transaction as a new transaction.

**NOTE:** When EOD is triggered, Provisional Reversals will be converted to Pending Reversals and will be processed as part of EOD.

#### **4.6.2. EMV Chip Card Declines**

If an EMV transaction is declined by an EMV card at first cryptogram generation (before communications) then the transaction is stored in a local file as a ChipCardDecline to be sent in the next online transaction (piggy backed). This is to inform the host of EMV chip declines for troubleshooting / helpdesk support.

#### **4.6.3. Signature uploads**

If a signature is captured for a transaction, it is stored as an AddAttachment message to be sent in the next online transaction (piggybacked).

**NOTE:** signature capture is only supported on the Lane/5000 terminal.

#### **4.6.4. SAF Transactions**

Store and Forward transactions are piggybacked onto the next online transaction as discussed in the next section.

## 4.7. SAF Transactions

Generally speaking, Store and Forward (SAF) processing is used when a communication failure prevents sending an authorization request to Portico. The merchant accepts the risk of storing the transaction for later transmission to Portico.

SAF transactions are stored in a local transaction file and piggybacked onto the next online transaction. To minimize delays in processing the next online transaction, only one SAF is piggybacked onto the next online transaction. All remaining SAF transactions are sent to the host when POS sends a SendSAF or EOD command to the SIP device.

If the SAF is declined, then it is marked as declined in the local transaction file. If an invalid response is received, then depending on the gateway error code it can be either marked as declined or it will remain in the local transaction file for retry. If a response is not received, then it will remain in the local transaction file for retry. More details on SAF retry are discussed in the [SAF Retries](#) section.

If partially approved, it is marked as partially approved.

### 4.7.1. SAF Modes

HPA supports three SAF modes per the **STORMD** parameter:

- **0 (OFF)**: In this mode, all transactions are declined if the host is not reachable. No transactions are stored offline as SAFs.
- **1 (ALWAYS)**: In this mode, all transactions are stored offline as SAFs if they pass the SAF Amount and Count limits. In SAF ALWAYS mode the SAFs are only sent to the host when SendSAF or EOD processing is initiated since there would not be an online transaction with which to piggyback the SAF.
- **3 (AUTO)**: In this mode, each transaction is attempted for host authorization. If it cannot reach the host, the transaction is stored offline as a SAF if they pass the SAF Amount and Count Limits.

### 4.7.2. SAF Amount Limit

A transaction will qualify for SAF if the transaction total amount is less than or equal to maximum SAF amount limit (**STORFL**).

### 4.7.3. SAF Count Limit

A transaction will qualify for SAF if the transaction count is less than or equal to the maximum SAF count limit (**STORLMT**).

#### 4.7.4. SAF Transaction States

- If a transaction is SAF approved and the response is successfully sent to the POS, HPA will mark the transaction as a **Pending SAF**, meaning that it is ready to be sent for deferred authorization as a piggyback or upon SendSAF or EOD.
- If a transaction is SAF approved but the response is not successfully sent to the POS, HPA will mark the transaction as a **Provisional SAF**, meaning that it has not yet been determined if it will be sent for deferred authorization.
  - If the next transaction from the POS is a resend (i.e. has the same <ECRId>, <Request> and <RequestId> elements as the previous transaction) then HPA will return the stored response for the previous transaction and mark the transaction as a Pending SAF.
  - If the next transaction from the POS is new (i.e. does not have the same <ECRId>, <Request> and <RequestId> elements as the previous transaction) then HPA will process the new transaction and mark the previous transaction as a **Discarded SAF**, meaning that it will not be sent for deferred authorization.
- Provisional and Discarded SAFs will not be sent to the host for deferred authorization as piggybacks or during SendSAF or EOD processing.
- Provisional and Discarded SAFs will not be considered in the SAF Count Limit as they are not sent in the SendSAF or EOD processing.
- When the EOD command is received, Provisional SAFs will be converted to Discarded SAFs.
- When the GetLastResponse command is received, and the last transaction was a Provisional SAF, it will be converted to a Pending SAF.

#### 4.7.5. SAF Eligible Transactions

The following transactions are eligible for Store and Forward:

- Credit Sale
- Credit Refund
- Voice Authorization
- Credit Auth
- Credit Additional Auth
- Credit Auth Complete
- Tip Adjust
- Transaction Adjust

**NOTE:** Transactions are not treated as SAF eligible when an online pin is entered, for example in SAF\_AUTO with an unreachable host.

## **4.7.6. SAF for Credit Auth/Additional Auth/Credit Auth Complete**

### **4.7.6.1. SAF Logic for Credit Auth**

If a comm failure occurs on a Credit Auth then assuming SAF is enabled the Credit Auth will be stored as SAF as long as the amount is below or equal to the SAF amount limit and the number of SAF transactions is below the SAF transaction count limit.

### **4.7.6.2. SAF Logic for Credit Additional Auth**

When a Credit Additional Auth transaction is received the SIP device checks if the original Credit Auth is SAF. If the Credit Auth is SAF, the sum of the original Credit Auth and Credit Additional Auth is compared with the SAF amount limit. If the sum is below or equal to the limit, then the amount of the Credit Auth is updated without going online. If the limit is exceeded the transaction is denied with EXCEEDS LIMIT response. The SAF transaction count limit is not checked since the Credit Auth transaction is updated without creating a new SAF.

If the original Credit Auth is not SAF the Credit Additional Auth is sent online. If a communication failure occurs the amount of the additional auth is compared with the SAF transaction limit and number of SAF transactions with total SAF transaction count limit. If neither limit is exceeded the Credit Additional Auth transaction is stored as SAF. If either limit is exceeded the transaction is denied with the EXCEEDS LIMIT response.

### **4.7.6.3. SAF Logic for Credit Auth Complete**

When a Credit Auth Complete transaction is received the SIP device checks if the original Credit Auth is SAF. If it is SAF the SAF amount limit is checked. If the amount is below or equal to the SAF amount limit the transaction is stored. If the amount exceeds the limit the transaction is denied with EXCEEDS LIMIT response. The SAF transaction count limit is not checked since Credit Auth/Auth Complete is effectively a single transaction.

If the original Credit Auth is not SAF the Credit Auth Complete is sent online. If a communication failure occurs the SAF transaction count is checked since the Credit Auth Complete is a new SAF. The SAF transaction amount limit is not checked as the authorization amount is presumed to have been authorized since the Credit Auth is not SAF. The SAF transaction count is not checked since the original credit auth was online approved, hence the transaction should not count against SAF limits.

It is a best practice for the Credit Auth Complete to not contain additional amounts that have not been previously authorized. Otherwise it is possible for the Credit Auth Complete to be stored as a SAF that exceeds the SAF amount limit.

## **4.7.7. EMV Chip Card Declines After Communications Failure**

If a communication failure prevents sending a CreditSale transaction for an EMV card, the application notifies the card that a communication failure occurred and requests the EMV card to approve the

transaction at the second cryptogram generation. The EMV card will then process the approval request based on the settings in the Terminal Verification Results (TVR) register and comparing them to the Terminal Action Default (TAC Default) and Issuer Action Default (IAC Default) registers. If the EMV card declines to approve the transaction offline, the decline is considered a “soft decline” and the transaction is processed as a SAF transaction. In this case the original ARQC is stored and sent in the CreditSale request when the SAF transactions are sent to Portico.

Note that if the EMV card approves the transaction offline after a communication failure, then the transaction is an offline approved transaction. A CreditOfflineSale transaction is stored and handled as an EMV Offline Approval Communication Failure.

#### **4.7.8. EMV and Voice Auth Offline Approval Communication Failures**

HPA now supports Quick Chip functionality. As part of Quick Chip offline approval of EMV transactions is no longer supported. Hence the following section is now deprecated.

If an EMV card approves a transaction offline at first cryptogram generation then the application will send the CreditOfflineSale message to Portico. If a communication failure occurs, then the transaction is treated as a SAF transaction.

Voice Auth transactions also use the same CreditOfflineSale message and are also stored in the case of communication failures.

**NOTE:** Offline Approvals are not treated as SAFs. A SAF transaction is a transaction for which the approval is pending until the authorization request is sent to the host, whereas Offline Approvals are approved transactions.

**NOTE:** Transactions that are offline approved by an EMV card after a communication failure are also stored in the local transaction file to be sent with the SAFs.

#### **4.7.9. Credit Adjustment and Void Support for SAF Transactions**

When a regular CreditSale request is authorized by Portico, the application returns the Gateway Transaction ID back to the POS in the Transaction ID element. The Transaction ID is needed to either adjust the transaction amount (i.e. add tip) or void the transaction.

If a POS requests a Credit Adjustment (Add Tip) or a Void for a transaction stored as a SAF transaction, then the application locates that transaction in the local transaction file, sends it to Portico, then uses the Gateway Transaction ID in the Portico response for the credit adjustment (CreditTxnEdit) or void (CreditVoid) transaction.

The reason for storing EMV Offline Approvals that have communication failures is to facilitate adjusting the amount or voiding the transaction. If the EMV Offline Approval were “piggybacked” on the next online connection, then the application would not be able to send the Gateway Transaction ID for the transaction back to the POS since it would happen on the next transaction.

Hence, if an EMV Offline Approved transaction has a communication failure, it is stored similar to a SAF. If the POS needs to adjust the amount or void the transaction, then the EMV Offline Approval can be located in the local transaction file and sent to the POS so that the application has the Gateway Transaction ID. Then the credit adjustment (CreditTXNEdit) or void (CreditVoid) transaction can be performed.

#### 4.7.10. SAF Reports

The POS may request a SAF Report with the GetSAF command. The SAF Report contains summary and detail information for pending and declined SAFs. Note that declined SAFs are kept in the local transaction file until the local transaction file is cleared during End Of Day processing. Hence if multiple GetSAF commands are performed before End Of Day processing, the same declined SAF transactions will be reported.

SAF reports are also generated during End Of Day processing. For these SAF Reports the reports include not only the pending and declined transactions but also the approved and partially approved transactions. Again these transactions remain in the local transaction file until the local transaction file is cleared during End Of Day processing.

#### 4.7.11. SAF Retries

Retry of pending SAF is performed on either the next online transaction as piggyback or on the next Send SAF or EOD command. Retry sending of pending SAF is done on the following conditions:

- No response from Portico. There is no limit on the number of retries until a response is received.
- Certain gateway response codes. Please refer to the table below:

Response Code	Description
-2	Authentication error
15	Batch close in progress
16	Invalid ship date
20	Database operation timeout
21	Archive database is currently unavailable
22	Archive database is currently unavailable but attempt was made to retrieve data from real-time database
30	Portico did not receive a response from the back-end system
31	Portico attempts a reversal for the POS but the reversal fails.



For retry because of certain gateway response codes:

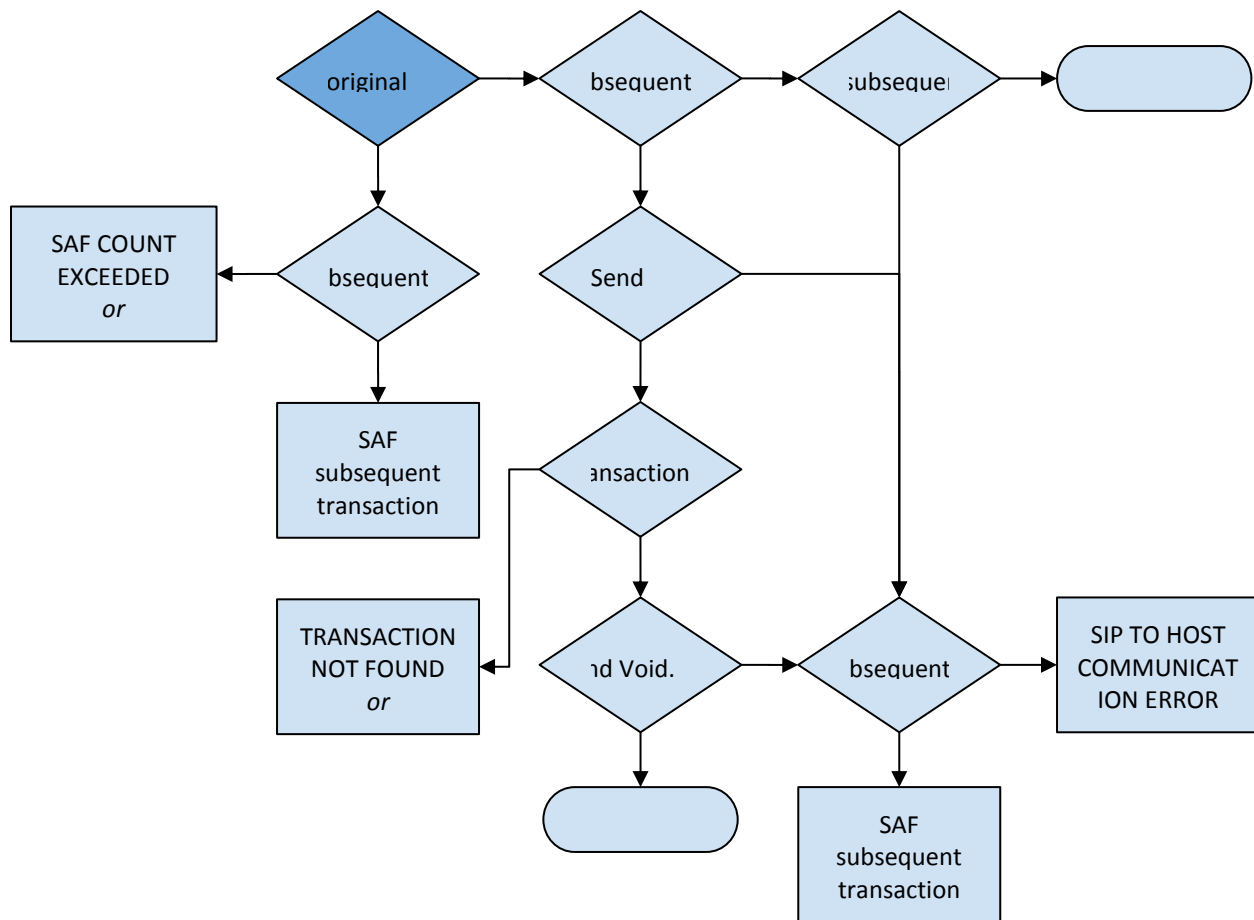
- A maximum retry count of 3 is implemented. When retry reaches max, the transaction is marked as declined in the local transaction file.
- When gateway response code is 30 or 31, a reversal is generated when transaction is to be marked as declined. The reversal is immediately sent.
- EOD will fail when at least 1 transaction is for retry or reversal fails.
- If reversal does not receive a response and fails, then the succeeding operation is stopped.

## 4.8. Subsequent Transactions

HPA supports sending the following subsequent transactions which modify the state of the original Sale or CreditAuth transaction using the Transaction ID from the original transaction:

- **Refund** - Refunds the full or partial amount of the original transaction.
- **Void** - Cancels the original transaction.
- **TipAdjust** - Adjusts the tip amount of the original transaction.
- **TransactionAdjust** - Adjusts the base and/or tip amount of the original transaction.
- **CreditAdditionalAuth** - Performs an additional authorization using the same card data as the original transaction.
- **CreditAuthComplete** - Adjusts the base and/or tip amount of the original transaction and adds it to the batch for settlement.

Subsequent transactions are processed as follows:



## 4.9. Bar Tab Processing Overview

HPA supports the following transactions needed for a POS to implement bar tab processing:

- CreditAuth:** A pre-authorization request used to open a tab. The CreditAuth transaction will place a hold on the cardholders account but will not be settled. The SIP device will prompt for card acquisition and send the authorization request to the Portico host. The CreditAuth response message includes the cardholder name when provided by the card so that it can be used to keep track of the tab.

**NOTE:** The POS is responsible for maintaining tab information, as that is not managed within HPA.

- CreditAdditionalAuth:** This transaction is used to perform an additional authorization on the card. Although it is possible to close the tab for a higher amount than the original preauthorization, there is no assurance that the higher amount will be approved. The recommended best practice is to perform additional auth transactions as needed to authorize the additional amount and ensure that the final amount will be approved.

- **CreditAuthComplete:** This transaction is used to close out a bar tab. The tab should be closed prior to End of Day processing to ensure that the transaction is included in the day's batch.

**NOTE:** If the tab is cancelled then a CreditVoid for the original CreditAuth should be done to clear the authorization hold on the cardholder's funds. If CreditAdditionalAuth transactions had been done, then Portico will automatically reverse them when the original CreditAuth is voided.

#### 4.9.1. CreditIncrementalAuth and CreditAdditionalAuth Differences

The Portico Host supports two similar transactions for doing a subsequent authorization to increase the amount of a previous pre-authorization:

- **CreditIncrementalAuth:** Used to increase the pre-authorization for Lodging merchants
- **CreditAdditionalAuth:** Used for additional pre-authorizations for Restaurant merchants

Although the functionality is similar, they differ in the amount of chargeback protection for the merchants.

The CreditIncrementalAuth is a true incremental authorization that increases the amount of the previous pre-authorization. Hence, the CreditIncrementalAuth provides chargeback protection for the increased authorization.

The CreditAdditionalAuth simply does a separate authorization request. The authorization request provides assurance to the merchant that the cardholder has additional credit available. When the transaction is added to the batch the previous additional authorizations are automatically reversed by the host. Hence the final CreditAuthComplete must specify the final total amount including the additional authorizations. Since only the additional authorizations are reversed the only chargeback protection is for the original CreditAuth.

More importantly, chargebacks may be initiated by the issuer if the final amount exceeds twenty percent of the original pre-authorization. If the final amount exceeds the twenty percent threshold charge protection is provided by voiding the original CreditAuth and performing a new CreditAuth for the final amount.

At the present time HPA doesn't support lodging and the Portico host doesn't support CreditIncrementAuth for restaurants. HPA does support restaurants so the CreditAdditionalAuth transaction is supported.

Integrators should be aware that while CreditAdditionalAuth doesn't have chargeback protection it does verify that the cardholder has the additional credit available.

Future releases of HPA will support a CreditIncrementalAuth when the Portico CreditIncrementalAuth functionality is expanded from lodging to retail/restaurant merchants.

## **4.10. Reboot Recommendation**

Due to PCI compliance requirements it is strongly recommended that the terminal be rebooted daily.

## **4.11. Contactless Transaction Support**

In accordance with card brand requirements HPA no longer supports Magstripe Mode/Magstripe Data (MSD) Contactless for Visa, MasterCard, and Discover. MSD Contactless is still supported for American Express (assuming the merchant accepts American Express).

If EMV is disabled then all contactless transactions including American Express MSD are disabled.

## 5. API Message Definition

The HPA API supports a wide range of financial transactions as well as a comprehensive set of manager functions and reports. All commands from the POS to the SIP device and the command responses from the SIP device to the POS are in XML. The XML rules, commands and their responses are defined below.

### 5.1. XML Syntax

The syntax rules of XML are very simple and logical. The definitions and rules are provided below for POS to/from HPA communications.

#### 5.1.1. Overview

The message format is based on XML. A set of XML elements is used to define both the request and the response messages between the POS and the SIP device.

#### 5.1.2. Rules

- For ease of integration, the XML elements are case insensitive. So <Mode> is the same as <MODE> and <mode>.
- White space is ignored except in the element and attribute values.
- The amount values should not have commas or decimals. So \$123.45 is sent as 12345.
- All amounts are positive. Credit and Debits are based on the transaction processed.
- Standard XML escape sequences are supported.
- Empty element shorthand is not allowed. So <Amount>12345</> is invalid. <Amount>12345</Amount> is valid.
- Elements are processed in any order. There is no defined order.
- XML must be in the correct format. However, the SIP device just looks for elements (custom XML processing) so it may not check for all XML format issues.
- If the XML request is incorrect - for example, if the <Request> element is missing, HPA may not respond. If there is no response from HPA, it is suggested to review the request message, and make sure it is accurate.
- UTF-8 character set is supported.
- Binary data such as signature data is sent using Hex ASCII.

## 5.2. Admin Commands

Admin commands are used for all actions not directly related to payments.

- Admin commands work only in a “Lane Closed” state.
- HPA will display “PROCESSING” while processing an Admin command.
- After the Admin command is processed, HPA will go back to the “Lane Closed” state.
- If used in a “Lane Opened” state, SIP device will respond with a “CANNOT PROCESS IN A LANE OPEN STATE” error response.
- While processing an Admin command, all other commands are responded with a “SIP DEVICE BUSY” error response.

**DISCLAIMER:** The Request and Response messages below are EXAMPLES ONLY, and may not contain all possible XML elements that can be sent to or received from HPA. Refer to the schema for a complete list of XML elements that may be included.

### 5.2.1. CloseBatch Command

This command is no longer supported. Batch Close functionality is part of the EOD process. If the **BATCHCLOSE** parameter is set then the EOD will close the batch with Portico.

Portico has the ability to auto-close the batch at a specific time, merchants should either enable Portico auto close or set **BATCHCLOSE** for the terminal to close the batch as part of EOD.

### 5.2.2. Download Command

This command downloads an application from HUDS as specified by the Terminal ID and the Application ID.

If more than one Application ID is associated with the Terminal ID then leaving the Application ID blank will result in all of the applications associated with those Application IDs to be downloaded. Additional applications include the Downloader application and SIP device firmware.

If a FULL download is specified then the application(s) will be downloaded. If PARTIAL download is specified then only the parameters associated with the Terminal ID will be downloaded. If DIFFERENTIAL download is specified, the Downloader first performs a partial download to get manifest files for Application Ids associated with the Terminal Id. Then the manifest files downloaded are compared with the inventory file stored on the terminal. The inventory file has all the information on the files downloaded previously to the terminal. If items in any manifest files do not match the counterparts in the inventory file, a FULL download to the Application Ids associated to those manifest files will be performed. And the inventory file will be updated accordingly after the download is successful.

**NOTE:** A download will remove any locally stored data, including stored SAF transactions, reversals, and signature attachments. End of Day processing should be run prior to any download to ensure all data has been sent to the host.

**NOTE:** When downloading a new version of HPA, the <ApplicationId> element should not be specified to ensure that the package containing the firmware and the Downloader application is also downloaded and installed.

**NOTE:** If the <HUDSURL> and/or <HUDSPORT> elements are not specified, the DOWNLOAD HOST URL (DLHOSTURL) and/or DOWNLOAD HOST PORT (DLPORT) parameters will be used instead.

### 5.2.2.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>Download</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<HUDSURL>	1-32X	Optional	See <a href="#">&lt;HUDSURL&gt;</a>
<HUDSPORT>	1-4N	Optional	See <a href="#">&lt;HUDSPORT&gt;</a>
<TerminalId>	1-8X	Mandatory	See <a href="#">&lt;TerminalId&gt;</a>
<ApplicationId>	1-20X	Optional	See <a href="#">&lt;ApplicationId&gt;</a>
<DownloadType>	1-7X	Mandatory	See <a href="#">&lt;DownloadType&gt;</a>
<DownloadTime>	1-14X	Mandatory	See <a href="#">&lt;DownloadTime&gt;</a>
</SIP>		Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.2.2.2. Request Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>Download</Request>
  <RequestId>10046</RequestId>
  <HUDSURL>SSLHPS.TEST.HPSDNL.D.NET</HUDSURL>
  <HUDSPORT>8001</HUDSPORT>
```

```

    <TerminalID>EB25033M</TerminalID>
    <ApplicationID>PI8HD33M</ApplicationID>
    <DownloadType>FULL</DownloadType>
    <DownloadTime>NOW</DownloadTime>
  </SIP>

```

### 5.2.2.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>Download</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<Responseld>	1-10N	Mandatory	See <a href="#">&lt;Responseld&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.2.2.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>10046</RequestId>
  <Response>Download</Response>

```



```
<ResponseId>10046</ResponseId>
<MultipleMessage>0</MultipleMessage>
<Result>0</Result>
<ResultText>Success</ResultText>
</SIP>
```

### 5.2.3. EOD Command

The EOD (End of Day) processing command is used to initiate the end of day processing from the POS. During EOD, any stored offline transactions (Pending SAF, attachments and reversals) are uploaded to the host.

The request format and the corresponding response are as shown in the following two subsections.

The response will denote with the status of each transaction as (SUCCESS/FAIL/NOT APPLICABLE).

Transactions supported are REVERSAL, OFFLINE DECLINE, TRANSACTION CERTIFICATE, ADD ATTACHMENT, SENDSAF, BATCH CLOSE, EMV PDL and HEARTBEAT.

**NOTE:** HPA will return **SIP DEVICE BUSY** error response for any POS command received while End of Day (EOD) process in progress.

#### 5.2.3.1. Initiation

End of day processing can be initiated either by

- An explicit EOD command. It can be sent at will by the POS, as many times as needed but typically once a day at the close of business.
- Automatically according to the End of Day timer, once every day if EODAUTO parameter is enabled/set to 1. The EODTIMER is a parameter in HPA that is set at TID level by WebTOPs. WebTOPs will set this timer to 20 minutes before Portico auto close time or some other desired time if Portico is not set to auto close. If there is no EODTIMER parameter or if the value is invalid, HPA will set EODTIMER to 11:00 PM (default).

Once initiated, the EOD logic will process the following in the order described below.

#### 5.2.3.2. Offline Transaction Processing

Any of the following transactions can be stored in the SIP devices that are offline processed. These transactions are normally piggybacked onto the next online transaction. However, if any of these have not yet been sent to the host then are sent up as part of EOD processing.

**NOTE:** Since the introduction of Quick Chip, EMV transactions are no longer approved offline. While EMV Offline Approvals should no longer occur, Offline Declines are still possible at the first cryptogram generation.

- Reversals
- Add Attachments (signatures)
- Store and Forward transactions (including credit sale, credit refund, and voice auth).
- EMV Offline Declines: These messages are sent to the Heartland host for troubleshooting purposes.

#### 5.2.3.3. Batch Close Processing

A batch close will be sent to Portico if **BATCHCLOSE** parameter is set to 1. If Portico is set to host auto close, this parameter should be set to 0 so HPA does not close the batch during EOD. If Portico is not set not for host auto close, this parameter should be set to 1 so HPA closes the batch during EOD.

#### 5.2.3.4. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>EOD</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.3.5. Request Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>EOD</Request>
  <RequestId>1004312</RequestId>
</SIP>
```

#### 5.2.3.6. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>

<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Conditional If returned by host.	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>EOD</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<Reversal>	1-32X	Mandatory	See <a href="#">&lt;Reversal&gt;</a>
<EMVOfflineDecline>	1-32X	Mandatory	See <a href="#">&lt;EMVOfflineDecline&gt;</a>
<TransactionCertificate>	1-32X	Mandatory	See <a href="#">&lt;TransactionCertificate&gt;</a>
<Attachment>	1-32X	Mandatory	See <a href="#">&lt;Attachment&gt;</a>
<SendSAF>	1-32X	Mandatory	See <a href="#">&lt;SendSAF&gt;</a>
<BatchClose>	1-32X	Mandatory	See <a href="#">&lt;BatchClose&gt;</a>
<HeartBeat>	1-32X	Mandatory	See <a href="#">&lt;HeartBeat&gt;</a>
<EMVPDL>	1-32X	Mandatory	See <a href="#">&lt;EMVPDL&gt;</a>
<EODStartTime>	12N	Mandatory	See <a href="#">&lt;EODStartTime&gt;</a>
<EODEndTime>	12N	Mandatory	See <a href="#">&lt;EODEndTime&gt;</a>
</SIP>		Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.2.3.7. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>

```

```

<DeviceId>6225529</DeviceId>
<RequestId>1004145</RequestId>
<Response>Reversal</Response>
<ResponseId>1004145</ResponseId>
<MultipleMessage>1</MultipleMessage>
<Result>0</Result>
<ResultText>NO REVERSAL NEEDED TO BE SENT</ResultText>
</SIP>

```

**NOTE:** Expect similar XML for the remaining EOD messages until the last message, below, where the RequestId remains the same for each EOD message.

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004145</RequestId>
  <Response>EOD</Response>
  <ResponseId>1024845791</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <Reversal>NO REVERSAL NEEDED TO BE SENT</Reversal>
  <EMVOfflineDecline>NO EMV OFFLINE DECLINE NEEDED TO BE SENT
</EMVOfflineDecline>
  <TransactionCertificate>NO EMV TC NEEDED TO BE SENT
</TransactionCertificate>
  <Attachment>SUCCESS</Attachment>
  <SendSAF>SUCCESS</SendSAF>
  <BatchClose>BATCH CLOSE SENT</BatchClose>
  <HeartBeat>HEART BEAT IS DISABLED</HeartBeat>
  <EMVPDL>NO EMV PARAMETERS TO DOWNLOAD</EMVPDL>
  <EODStartTime>060419091151</EODStartTime>
  <EODEndTime>060419091231</EODEndTime>
</SIP>

```

**NOTE:** SIP Device will reboot after every successful EOD processing whether EOD initiated explicitly by POS command or automatically by timed event. **EOD Command**

The EOD (End of Day) processing command is used to initiate the end of day processing from the POS. During EOD, any stored offline transactions (Pending SAF, attachments and reversals) are uploaded to the host.

The request format and the corresponding response are as shown in the following two subsections.

The response will denote with the status of each transaction as (SUCCESS/FAIL/NOT APPLICABLE).

Transactions supported are REVERSAL, OFFLINE DECLINE, TRANSACTION CERTIFICATE, ADD ATTACHMENT, SENDSAF, BATCH CLOSE, EMV PDL and HEARTBEAT.

**NOTE:** HPA will return **SIP DEVICE BUSY** error response for any POS command received while End of Day (EOD) process in progress.

#### 5.2.3.8. Initiation

End of day processing can be initiated either by

- An explicit EOD command. It can be sent at will by the POS, as many times as needed but typically once a day at the close of business.
- Automatically according to the End of Day timer, once every day if EODAUTO parameter is enabled/set to 1. The EODTIMER is a parameter in HPA that is set at TID level by WebTOPs. WebTOPs will set this timer to 20 minutes before Portico auto close time or some other desired time if Portico is not set to auto close. If there is no EODTIMER parameter or if the value is invalid, HPA will set EODTIMER to 11:00 PM (default).

Once initiated, the EOD logic will process the following in the order described below.

#### 5.2.3.9. Offline Transaction Processing

Any of the following transactions can be stored in the SIP devices that are offline processed. These transactions are normally piggybacked onto the next online transaction. However, if any of these have not yet been sent to the host then are sent up as part of EOD processing.

**NOTE:** Since the introduction of Quick Chip, EMV transactions are no longer approved offline. While EMV Offline Approvals should no longer occur, Offline Declines are still possible at the first cryptogram generation.

- Reversals
- Add Attachments (signatures)
- Store and Forward transactions (including credit sale, credit refund, and voice auth).
- EMV Offline Declines: These messages are sent to the Heartland host for troubleshooting purposes.

#### 5.2.3.10. Batch Close Processing

A batch close will be sent to Portico if **BATCHCLOSE** parameter is set to 1. If Portico is set to host auto close, this parameter should be set to 0 so HPA does not close the batch during EOD. If Portico is not set not for host auto close, this parameter should be set to 1 so HPA closes the batch during EOD.

### 5.2.3.11. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>EOD</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.2.3.12. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>EOD</Request>
  <RequestId>1004312</RequestId>
</SIP>

```

### 5.2.3.13. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Conditional If returned by host.	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>EOD</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>

<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<Reversal>	1-32X	Mandatory	See <a href="#">&lt;Reversal&gt;</a>
<EMVOfflineDecline>	1-32X	Mandatory	See <a href="#">&lt;EMVOfflineDecline&gt;</a>
<TransactionCertificate>	1-32X	Mandatory	See <a href="#">&lt;TransactionCertificate&gt;</a>
<Attachment>	1-32X	Mandatory	See <a href="#">&lt;Attachment&gt;</a>
<SendSAF>	1-32X	Mandatory	See <a href="#">&lt;SendSAF&gt;</a>
<BatchClose>	1-32X	Mandatory	See <a href="#">&lt;BatchClose&gt;</a>
<HeartBeat>	1-32X	Mandatory	See <a href="#">&lt;HeartBeat&gt;</a>
<EMVPDL>	1-32X	Mandatory	See <a href="#">&lt;EMVPDL&gt;</a>
<EODStartTime>	12N	Mandatory	See <EODStartTime>
<EODEndTime>	12N	Mandatory	See <EODEndTime>
</SIP>		Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.3.14. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004145</RequestId>
  <Response>Reversal</Response>
  <ResponseId>1004145</ResponseId>
  <MultipleMessage>1</MultipleMessage>
  <Result>0</Result>
  <ResultText>NO REVERSAL NEEDED TO BE SENT</ResultText>
</SIP>

```

**NOTE:** Expect similar XML for the remaining EOD messages until the last message, below, where the RequestId remains the same for each EOD message.

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004145</RequestId>
  <Response>EOD</Response>
  <ResponseId>1024845791</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <Reversal>NO REVERSAL NEEDED TO BE SENT</Reversal>
  <EMVOfflineDecline>NO EMV OFFLINE DECLINE NEEDED TO BE SENT
</EMVOfflineDecline>
  <TransactionCertificate>NO EMV TC NEEDED TO BE SENT
</TransactionCertificate>
  <Attachment>SUCCESS</Attachment>
  <SendSAF>SUCCESS</SendSAF>
  <BatchClose>BATCH CLOSE SENT</BatchClose>
  <HeartBeat>HEART BEAT IS DISABLED</HeartBeat>
  <EMVPDL>NO EMV PARAMETERS TO DOWNLOAD</EMVPDL>
  <EODStartTime>060419091151</EODStartTime>
  <EODEndTime>060419091231</EODEndTime>
</SIP>

```

**NOTE:** SIP Device will reboot after every successful EOD processing whether EOD initiated explicitly by POS command or automatically by timed event.

## 5.2.4. GetAppInfoReport Command

This command will return the HPA Application Info from the SIP device to the POS. HPA will display "PROCESSING".

### 5.2.4.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>GetAppInfoReport</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>



### 5.2.4.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>GetAppInfoReport</Request>
  <RequestId>1004112</RequestId>
</SIP>

```

### 5.2.4.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>GetAppInfoReport</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
<TableCategory>	See <a href="#">Record Data</a>	Conditional If new category of elements begin	See <a href="#">&lt;TableCategory&gt;</a>
<Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>
<Key>	See <a href="#">Record Data</a>	Mandatory	See <a href="#">&lt;Key&gt;</a>
<Value>	See <a href="#">Record Data</a>	Mandatory	See <a href="#">&lt;Value&gt;</a>
</Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>

...	--	--	<Field>, <Key>, <Value>, and </Field> elements repeat as specified for each Record/TableCategory per <a href="#">Record Data</a>
</Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.4.4. Record Data

<TableCategory>	<Key>	<Value>	Usage
GENERAL INFORMATION	APPLICATION	8X	Mandatory
	VERSION	13-14X (X.X.X.XXXXXXXXXX)	Mandatory
	APPLICATION MODE	5-10X	Mandatory
	REV	7-8X	Mandatory
	COPYRIGHT (c)	9X	Mandatory
	HEARTLAND PAYMENT SYSTEMS, INC.	1-32X	Mandatory
DOWNLOADER INFORMATION	VERSION	13-14X (X.X.X.XXXXXXXXXX)	Mandatory
	APPLICATION ID	1-20X	Mandatory
	TERMINAL ID	1-20X	Mandatory
TERMINAL INFORMATION	SDK RELEASE	1-4N.NN.N	Mandatory
	TELIUM MANAGER	1-4N	Mandatory
	TELIUM SYSTEM	1-4N	Mandatory
	HARDWARE TYPE	1-32X	Mandatory
	SERIAL NUMBER	1-32X	Mandatory
	INJECTED NUMBER	1-32N	Mandatory

	APPLICATION ID	1-20X	Mandatory
	TERMINAL ID	1-20X	Mandatory
	CURRENT TIME	1-14N	Mandatory
	BATTERY LEVEL	--	Mandatory
IP INFORMATION	MAC ADDRESS	1-17X	Mandatory
	TCP MODULE	1-9N	Mandatory
	USE DHCP?	1N	Mandatory
	TERMINAL IP	NNN.NNN.NNN.NNN	Mandatory
	SUBNET MASK	NNN.NNN.NNN.NNN	Mandatory
	GATEWAY IP	NNN.NNN.NNN.NNN	Mandatory
	PRIMARY DNS	NNN.NNN.NNN.NNN	Mandatory
	SECONDARY DNS	NNN.NNN.NNN.NNN	Mandatory
MEMORY INFORMATION	INTERNAL RAM TOTAL	1-10N	Mandatory
	INTERNAL RAM USED	1-10N	Mandatory
	PERCENT RAM USED	1-3N	Mandatory
	INTERNAL RAM AVAILABLE	1-10N	Mandatory
	BATCH RECORD COUNT	1-10N	Mandatory
	MAX BATCH COUNT	1-3N	Mandatory
	PERCENT USED BATCH	1-3N	Mandatory
	FLASH RAM TOTAL	1-10N	Mandatory
	FLASH RAM USED	1-8N	Mandatory
	FLASH RAM AVAILABLE	1-10N	Mandatory
	BATCH RECORD SIZE	1-10N	Mandatory
HEARTLAND LIBRARIES	BATCH LIBRARY	1-12N.N.NNNN	Mandatory

BIN CONFIG LIBRARY	1-12N.N.NNNN	Mandatory
CARD READER LIBRARY	1-12N.N.NNNN	Mandatory
CHECK READER LIBRARY	1-12N.N.NNNN	Mandatory
DATA ENTRY LIBRARY	1-12N.N.NNNN	Mandatory
DISPLAY LIBRARY	1-12N.N.NNNN	Mandatory
E3 LIBRARY	1-12N.N.NNNN	Mandatory
MENU LIBRARY	1-12N.N.NNNN	Mandatory
MSG PARSE LIBRARY	1-12N.N.NNNN	Mandatory
MODEM LIBRARY	1-12N.N.NNNN	Mandatory
PARAMETER LIBRARY	1-12N.N.NNNN	Mandatory
PIN PAD LIBRARY	1-12N.N.NNNN	Mandatory
PLATFORM LIBRARY	1-12N.N.NNNN	Mandatory
PRINTER LIBRARY	1-12N.N.NNNN	Mandatory
NFC READER LIBRARY	1-12N.N.NNNN	Mandatory
SCANNER LIBRARY	1-12N.N.NNNN	Mandatory
SERIAL LIBRARY	1-12N.N.NNNN	Mandatory
TCP/IP LIBRARY	1-12N.N.NNNN	Mandatory
TIMED EVENT LIBRARY	1-12N.N.NNNN	Mandatory
UI LIBRARY	1-12N.N.NNNN	Mandatory
UTILITY LIBRARY	1-12N.N.NNNN	Mandatory
VIRTUAL COM LIBRARY	1-12N.N.NNNN	Mandatory

#### 5.2.4.5. Response Example

Every <Record> in a response will have the following characteristics:

- A similar XML heading

- Table category followed by 30 or less <Field> elements or
- 30 or less <Field> elements with no TableCategory.

Essentially the presence of TableCategory as a first element in the response record indicates the beginning of a new category of elements and the table category descriptor gives a very short description of the category.

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004112</RequestId>
  <Response>GetAppInfoReport</Response>
  <ResponseId>1004112</ResponseId>
  <MultipleMessage>1</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <Record>
    <TableCategory>GENERAL INFORMATION</TableCategory>
    <Field>
      <Key>APPLICATION</Key>
      <Value>Heartland Payment App</Value>
    </Field>
    <Field>
      <Key>VERSION</Key>
      <Value>3.3.0</Value>
    </Field>
    <Field>
      <Key>APPLICATION MODE</Key>
      <Value>RETAIL</Value>
    </Field>
    <Field>
      <Key>REV</Key>
      <Value></Value>
    </Field>
    <Field>
      <Key>COPYRIGHT (c)</Key>
      <Value>1997-2018</Value>
    </Field>
    <Field>
      <Key>HEARTLAND PAYMENT SYSTEMS, INC.</Key>
      <Value>ALL RIGHTS RESERVED</Value>
    </Field>
    ...
  </Record>
</SIP>
```

### 5.2.5. GetBatchReport Command

This command will return the current Batch details from the SIP device to the POS.

HPA always returns both the batch summary and the batch detail report. Currently, HPA supports Batch Detail Report for up to 1000 Transactions. In case Batch holds more than 1000 transactions, Only Batch Summary Report is printed along with Message saying “Batch Detail Report is too large to print.”

#### 5.2.5.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>GetBatchReport</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<FieldCount>	1-2N	Optional	See <a href="#">&lt;FieldCount&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.5.2. Request Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>GetBatchReport</Request>
  <RequestId>1004117</RequestId>
</SIP>
```

#### 5.2.5.3. Summary Response

A batch summary request response will have a BatchReportHeader message followed by another message that will contain the CREDIT and DEBIT card summaries, and the transaction summary for EBT and GIFT cards. This message will conclude with transaction summaries of SALES, REFUNDS and VOID for the batch.

**NOTE:** Currently, Gift transactions are not returned in the Batch Report.

## 5.2.5.3.1. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>GetBatchReport</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
<TableCategory>	See <a href="#">Record Data</a>	Conditional If new category of elements begin	See <a href="#">&lt;TableCategory&gt;</a>
<Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>
<Key>	See <a href="#">Record Data</a>	Mandatory	See <a href="#">&lt;Key&gt;</a>
<Value>	See <a href="#">Record Data</a>	Mandatory	See <a href="#">&lt;Value&gt;</a>
</Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>
...	--	--	<Field>, <Key>, <Value>, and </Field> elements repeat as specified for each Record/TableCategory per <a href="#">Record Data</a>

</Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

## 5.2.5.3.2. Record Data

<TableCategory>	<Key>	<Value>	Usage
BATCH SUMMARY	MerchantName	1-32X	Mandatory
	Siteld	1-20X	Mandatory
	Deviceld	1-8N	Mandatory
	BatchId	1-3N	Mandatory
	BatchSeqNbr	1-4N	Mandatory
	BatchStatus	1X	Mandatory
	OpenUtcDT	14N	Mandatory
	CloseUtcDT	14N	Mandatory
	OpenTxnId	1-10N	Mandatory
	CloseTxnId	1-10N	Mandatory
	BatchTxnCnt	1-5N	Mandatory
	BatchTxnAmt	1-12N	Mandatory
	CreditCnt	1-5N	Mandatory
	CreditAmt	1-12X	Mandatory
	DebitCnt	1-5N	Mandatory
	DebitAmt	1-12X	Mandatory



Individual Card Summary e.g. VISA CARD SUMMARY	SaleCnt	1-5N	Mandatory
	SaleAmt	1-12X	Mandatory
	ReturnCnt	1-5N	Mandatory
	ReturnAmt	1-12X	Mandatory
	CardType	1-21X	Mandatory
	TransType	3-7X	Mandatory
	NumberTransactions	1-5N	Mandatory
	TotalAmount	1-12X	Mandatory

#### 5.2.5.3.3. Response Example

The Portico Response begins with two messages providing batch summary information followed by ten messages providing card summary information. The ten card summary messages consist of two messages each with card summary information each for Visa, MasterCard, American Express, and Discover.

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004117</RequestId>
  <Response>GetBatchReport</Response>
  <ResponseId>1024812786</ResponseId>
  <MultipleMessage>1</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <Record>
    <TableCategory>BATCH SUMMARY</TableCategory>
    <Field>
      <Key>MerchantName</Key>
      <Value>PIF1938 RTL43</Value>
    </Field>
    <Field>
      <Key>SiteId</Key>
      <Value>122880</Value>
    </Field>
  </Record>

```

```

    <Field>
      <Key>DeviceId</Key>
      <Value>6225529</Value>
    </Field>
    <Field>
      <Key>BatchId</Key>
      <Value>434273</Value>
    </Field>
    <Field>
      <Key>BatchSeqNbr</Key>
      <Value>46</Value>
    </Field>
    <Field>
      <Key>BatchStatus</Key>
      <Value>OPEN</Value>
    </Field>
    <Field>
      <Key>OpenUtcDT</Key>
      <Value>2017-09-14T11:04:22.49Z</Value>
    </Field>
    <Field>
      <Key>CloseUtcDT</Key>
      <Value>
    </Value>
    </Field>
    <Field>
      <Key>OpenTxnId</Key>
      <Value>1024805970</Value>
    </Field>
    ...
  </Record>
</SIP>

```

#### 5.2.5.4. Detail Response

A batch detail request response will have a BatchReportHeader message followed by one SIP response message for each transaction giving the details of the transaction. HPA downloads the entire report from Portico before sending it to the POS. While the download is in progress, the POS cannot abort the process. The POS can only abort the flow in the second phase when the report is being sent.

##### 5.2.5.4.1. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>

<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>GetBatchReport</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
<TableCategory>	See Record Data	Conditional If new category of elements begin	See <a href="#">&lt;TableCategory&gt;</a>
<Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>
<Key>	See Record Data	Mandatory	See <a href="#">&lt;Key&gt;</a>
<Value>	See Record Data	Mandatory	See <a href="#">&lt;Value&gt;</a>
</Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>
...	--	--	<Field>, <Key>, <Value>, and </Field> elements repeat as specified for each Record/TableCategory per Record Data
</Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.5.4.2. Record Data

<TableCategory>	<Key>	<Value>	Usage
-----------------	-------	---------	-------

BATCH DETAIL	MerchantName	1-32X	Mandatory
	DeviceId	1-8N	Mandatory
	SiteId	1-20X	Mandatory
	BatchId	1-3N	Mandatory
	BatchSeqNbr	1-4N	Mandatory
	BatchStatus	1X	Mandatory
	OpenUtcDT	14N	Mandatory
	OpenTxnId	1-10N	Mandatory
	BatchTxnAmt	1-12N	Mandatory
	BatchTxnCnt	1-5N	Mandatory
Individual Transaction e.g. TRANSACTION 1 DETAIL	ReferenceNumber	4-16N	Mandatory
	TransactionTime	1-32X	Mandatory
	TransactionStatus <sup>1</sup>	1-32X	Mandatory
	MaskedPAN	15-19X	Mandatory
	CardType	16X	Mandatory
	TransactionType	3-7X	Mandatory
	CardAcquisition	7X	Mandatory
	ApprovalCode	6N	Mandatory
	Responsecode	2N	Mandatory

	ResponseText	16X	Mandatory
	CashbackAmount	1-7N	Mandatory
	TipAmount	1-6N	Mandatory
	AuthorizedAmount	1-7N	Mandatory
	SettleAmount	1-7N	Mandatory
	RequestedAmount	1-7N	Mandatory

#### 5.2.5.4.3. Response Example

HPA sends the following detail record, which is repeated for each transaction in the batch:

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100448</RequestId>
  <Response>GetBatchReport</Response>
  <MultipleMessage>1</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <Record>
    <TableCategory>TRANSACTION 1 DETAIL</TableCategory>
    <Field>
      <Key>ReferenceNumber</Key>
      <Value>1023802207</Value>
    </Field>
    <Field>
      <Key>TransactionTime</Key>
      <Value>2017-08-16T18:16:01.763Z</Value>
    </Field>
    <Field>
      <Key>TransactionStatus</Key>
      <Value>ACTIVE</Value>
    </Field>
    <Field>
      <Key>MaskedPAN</Key>
      <Value>401200*****0016</Value>
    </Field>
    <Field>
      <Key>CardType</Key>

```

```

    <Value>Visa</Value>
  </Field>
  <Field>
    <Key>TransactionType</Key>
    <Value>CreditSale</Value>
  </Field>
  <Field>
    <Key>CardAcquisition</Key>
    <Value>SWIPE</Value>
  </Field>
  <Field>
    <Key>ApprovalCode</Key>
    <Value>46203A</Value>
  </Field>
  <Field>
    <Key>ResponseCode</Key>
    <Value>00</Value>
  </Field>
  <Field>
    <Key>ResponseText</Key>
    <Value>APPROVAL</Value>
  </Field>
</Record>
</SIP>

```

### 5.2.6. GetEMVParameterReport Command

This command will return the EMV Parameter Download (PDL) data from the SIP device to the ECR.

#### 5.2.6.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	n/a	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>GetParameterReport</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<FieldCount>	1-2N	Optional	See <a href="#">&lt;FieldCount&gt;</a>

</SIP>		Mandatory	See <a href="#">&lt;SIP&gt;</a>
--------	--	-----------	---------------------------------

### 5.2.6.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>GetEMVParameterReport</Request>
  <RequestId>100424</RequestId>
  <FieldCount>30</FieldCount>
</SIP>

```

### 5.2.6.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>GetEMVParameterReport</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
<TableCategory>	See <a href="#">Record Data</a>	Conditional If new category of elements begin	See <a href="#">&lt;TableCategory&gt;</a>
<Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>
<Key>	See <a href="#">Record Data</a>	Mandatory	See <a href="#">&lt;Key&gt;</a>

<Value>	See <a href="#">Record Data</a>	Mandatory	See <a href="#">&lt;Value&gt;</a>
</Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>
...	--	--	<Field>, <Key>, <Value>, and </Field> elements repeat as specified for each Record/TableCategory per <a href="#">Record Data</a>
</Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.6.4. Record Data

<TableCategory>	<Key>	<Value>	Usage
TABLE 30 TERMINAL DATA	AddlTermCapabilities	1-10X	Mandatory
	TermCountryCode	3N	Mandatory
	TranCurrencyCode	3N	Mandatory
	TranCurrencyExponent	1N	Mandatory
	TranRefCurrencyCode	3N	Mandatory
	TranRefCurrencyExponent	1N	Mandatory
TABLE 40 RID CONTACT_DATA	RID	1N	Mandatory
	ContactData	1N	Mandatory
	AID	1-32X	Mandatory
	AppSelectionIndicator	N	Mandatory
	AppVersionNum	1-4X	Mandatory



	AppCountryCode	1-3N	Mandatory
	TransactionTypes	3-7X	Mandatory
	TermCapabilities	1-6X	Mandatory
	TermFloorLimit	1-12N	Mandatory
	RandomSelectionThreshold	1-12N	Mandatory
	RandomSelectionPercent	1-3N	Mandatory
	RandomSelectionPercentMax	1-3N	Mandatory
	TACDenial	1-10X	Mandatory
	TACOnline	1-10X	Mandatory
	TACDefault	1-10X	Mandatory
	TermRiskManagementData	1-16X	Mandatory
	TDOL	1-64X	Mandatory
	DDOL	1-64X	Mandatory
TABLE 50 RID CONTACTLESS_DATA	RID	1N	Mandatory
	ContactlessData	1N	Mandatory
	AID	1-32X	Mandatory
	AppSelectionIndicator	1N	Mandatory
	AppVersionNum	1-4X	Mandatory
	MagstripeAppVersionNum	1-4X	Mandatory

	AppCountryCode	1-3N	Mandatory
	TransactionTypes	3-7X	Mandatory
	TermCapabilities	1-6X	Mandatory
	TermFloorLimit	1-12N	Mandatory
	TermCVMLimit	1-12N	Mandatory
	TermTranLimit	1-12N	Mandatory
	TACDenial	1-10X	Mandatory
	TACOnline	1-10X	Mandatory
	TACDefault	1-10X	Mandatory
	TermRiskManagementData	1-16X	Mandatory
	TDOL	1-64X	Mandatory
	TermTranQualifiers	1-32X	Mandatory
TABLE 60 RID CAPK	RID	1N	Mandatory
	CAPK	1N	Mandatory
	RID	1-10X	Mandatory
	Index	1-2X	Mandatory
	Status	1X	Mandatory
	ModulusLength	1-3N	Mandatory
	Exponent	1N	Mandatory

	Checksum	1-40X	Mandatory
--	----------	-------	-----------

### 5.2.6.5. Response Example

Every <Record> in a response will have the following characteristics:

- A similar XML heading
- Table category followed by 30 or less <Field> elements or
- 30 or less <Field> elements with no TableCategory.

Essentially the presence of TableCategory as a first element in the response record indicates the beginning of a new category of elements and the table category descriptor gives a very short description of the category.

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100424</RequestId>
  <Response>GetEMVParameterReport</Response>
  <ResponseId>100424</ResponseId>
  <MultipleMessage>1</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <Record>
    <TableCategory>TABLE 30 TERMINAL DATA</TableCategory>
    <Field>
      <Key>AddlTermCapabilities</Key>
      <Value>7000F0B001</Value>
    </Field>
    <Field>
      <Key>TermCountryCode</Key>
      <Value>840</Value>
    </Field>
    <Field>
      <Key>TranCurrencyCode</Key>
      <Value>840</Value>
    </Field>
    <Field>
      <Key>TranCurrencyExponent</Key>
      <Value>2</Value>
    </Field>
    <Field>
      <Key>TranRefCurrencyCode</Key>
```

```

        <Value>840</Value>
    </Field>
    <Field>
        <Key>TranRefCurrencyExponent</Key>
        <Value>2</Value>
    </Field>
    ...
</Record>
</SIP>

```

### 5.2.7. GetLastEODReport Command

The GetLastEODReport command is used to initiate the reprint of last End of Day report from the POS.

The request format and the corresponding response are as shown in the following two subsections. The response will denote the status of transaction as SUCCESS or FAIL.

**NOTE:** For this command to get the batch report as part of EOD the batch must be closed at the terminal rather than Auto Close at Portico.

**NOTE:** The Last EOD report will return with all the original fields except for <RequestId> which will match the current request. Only the final response packet for the GetLastEODReport command should contain the identifiers of the requesting device.

#### 5.2.7.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>GetLastEODReport</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.7.2. Request Example

```

<SIP>
    <Version>1.0</Version>
    <ECRId>1004</ECRId>
    <Request>GetLastEODReport</Request>
    <RequestId>1004312</RequestId>
</SIP>

```

## 5.2.7.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<Deviceld>	1-8N	Conditional If returned by host.	See <a href="#">&lt;Deviceld&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>GetLastEODReport</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<Responseld>	4-16N	Mandatory	See <a href="#">&lt;Responseld&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<Reversal>	1-32X	Mandatory	See <a href="#">&lt;Reversal&gt;</a>
<EMVOfflineDecline>	1-32X	Mandatory	See <a href="#">&lt;EMVOfflineDecline&gt;</a>
<TransactionCertificate>	1-32X	Mandatory	See <a href="#">&lt;TransactionCertificate&gt;</a>
<Attachment>	1-32X	Mandatory	See <a href="#">&lt;Attachment&gt;</a>
<SendSAF>	1-32X	Mandatory	See <a href="#">&lt;SendSAF&gt;</a>
<BatchClose>	1-32X	Mandatory	See <a href="#">&lt;BatchClose&gt;</a>
<HeartBeat>	1-32X	Mandatory	See <a href="#">&lt;HeartBeat&gt;</a>
<EMVPDL>	1-32X	Mandatory	See <a href="#">&lt;EMVPDL&gt;</a>
<EODStartTime>	12N	Mandatory	See <EODStartTime>
<EODEndTime>	12N	Mandatory	See <EODEndTime>

</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
--------	----	-----------	---------------------------------

#### 5.2.7.4. Response Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004145</RequestId>
  <Response>Reversal</Response>
  <ResponseId>1004145</ResponseId>
  <MultipleMessage>1</MultipleMessage>
  <Result>0</Result>
  <ResultText>NO REVERSAL NEEDED TO BE SENT</ResultText>
</SIP>
```

**NOTE:** Expect similar XML for the remaining GetEODReport messages until the last message, below, where the RequestId remains the same for each message.

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004145</RequestId>
  <Response>GetLastEODReport</Response>
  <ResponseId>1024845791</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <Reversal>NO REVERSAL NEEDED TO BE SENT</Reversal>
  <EMVOfflineDecline>NO EMV OFFLINE DECLINE NEEDED TO BE SENT</EMVOfflineDecline>
  <TransactionCertificate>NO EMV TC NEEDED TO BE SENT</TransactionCertificate>
  <Attachment>SUCCESS</Attachment>
  <SendSAF>SUCCESS</SendSAF>
  <BatchClose>BATCH CLOSE SENT</BatchClose>
  <HeartBeat>HEART BEAT IS DISABLED</HeartBeat>
  <EMVPDL>NO EMV PARAMETERS TO DOWNLOAD</EMVPDL>
  <EODStartTime>060419091151</EODStartTime>
  <EODEndTime>060419091231</EODEndTime>
</SIP>
```

## 5.2.8. GetLastResponse Command

This command is used to retrieve the last financial transaction performed which can be either successful or failed. This command will work in both “Lane Closed” and “Lane Opened” states.

### 5.2.8.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>GetLastResponse</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
</SIP>		Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.2.8.2. Request Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>GetLastResponse</Request>
  <RequestId>100417</RequestId>
</SIP>
```

### 5.2.8.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>

<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>GetLastResponse</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	1-10N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<LastResponse>	NA	Mandatory	See <a href="#">&lt;LastResponse&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.8.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100417</RequestId>
  <Response>GetLastResponse</Response>
  <ResponseId>100417</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <LastResponse>
    <Version>1.0</Version>
    <ECRId>1004</ECRId>
    <SIPIId>16322SC81188236</SIPIId>
    <DeviceId>6225529</DeviceId>
    <RequestId>100410</RequestId>
    <Response>Sale</Response>
    <ResponseId>1024541600</ResponseId>
    <MultipleMessage>0</MultipleMessage>
    <Result>0</Result>
    <ResultText>Success</ResultText>
    <TransactionTime>090817041937</TransactionTime>
    <GatewayRspCode>0</GatewayRspCode>
    <GatewayRspMsg>Success</GatewayRspMsg>
    <ResponseCode>00</ResponseCode>
  </LastResponse>
</SIP>

```



```

    <ResponseText>APPROVAL</ResponseText>
    <ApprovalCode>019883</ApprovalCode>
    <ReferenceNumber>725113882553</ReferenceNumber>
    <CardType>MASTERCARD</CardType>
    <CardGroup>CREDIT</CardGroup>
    <CardAcquisition>MSD TAP</CardAcquisition>
    <MaskedPAN>*****4111</MaskedPAN>
    <SignatureLine>0</SignatureLine>
    <PinVerified>0</PinVerified>
    <TipAdjustAllowed>1</TipAdjustAllowed>
    <QPSQualified>0</QPSQualified>
    <AdditionalTipAmount>0</AdditionalTipAmount>
    <TipAmount>10</TipAmount>
    <TaxAmount>20</TaxAmount>
    <AuthorizedAmount>229</AuthorizedAmount>
    <TokenRspCode>0</TokenRspCode>
    <TokenRspMsg>Success</TokenRspMsg>
    <TokenValue>JP21fN08Ed4QA9WkA14C0016</TokenValue>
    <StoredResponse>1</StoredResponse>
  </LastResponse>
</SIP>

```

### 5.2.9. GetParameterReport Command

This command will return the current parameter settings (KEY/VALUE pairs, one pair at a time) from the SIP device to the POS.

#### 5.2.9.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	n/a	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>GetParameterReport</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<FieldCount>	1-2N	Optional	See <a href="#">&lt;FieldCount&gt;</a>
</SIP>		Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.2.9.2. Request Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>GetParameterReport</Request>
  <RequestId>10042</RequestId>
  <FieldCount>30</FieldCount>
</SIP>
```

### 5.2.9.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>GetParameterReport</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
<TableCategory>	See <a href="#">Record Data</a>	Conditional If new category of elements begin	See <a href="#">&lt;TableCategory&gt;</a>
<Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>
<Key>	See <a href="#">Record Data</a>	Mandatory	See <a href="#">&lt;Key&gt;</a>
<Value>	See <a href="#">Record Data</a>	Mandatory	See <a href="#">&lt;Value&gt;</a>
</Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>

...	--	--	<Field>, <Key>, <Value>, and </Field> elements repeat as specified for each Record/TableCategory per <a href="#">Record Data</a>
</Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.9.4. Record Data

<TableCategory>	<Key>	<Value>	Usage
CARD TYPE PARAMETERS	BEGINNING BIN	1-19N	Mandatory
	ENDING BIN	1-19N	Mandatory
	ENABLED	B	Mandatory
	LONG CARD NAME	1-16X	Mandatory
	SHORT CARD NAME	1-3X	Mandatory
	CARD TYPE	1-2N	Mandatory
	MIN LENGTH	1-2N	Mandatory
	MAX LENGTH	1-2N	Mandatory
	ALLOW MANUAL	B	Mandatory
	CHECK AVS	B	Mandatory
	SECURITY CODE	B	Mandatory
	CHECK EXP DATE	B	Mandatory
	ALLOW CASHBACK	B	Mandatory

COMMUNICATION TYPE PARAMETERS	ALLOW TIP	B	Mandatory
	TIP DISCOUNT	1-2N	Mandatory
	QPS LIMIT	4N	Mandatory
	CHECK LUHN	B	Mandatory
	PRIMARY AUTH URL	128X	Mandatory
	PRIMARY AUTH PORT	1-5N	Mandatory
	PRIMARY SETTLE URL	128X	Mandatory
	PRIMARY SETTLE PORT	1-5N	Mandatory
	PRIMARY HGM URL	128X	Mandatory
	PRIMARY HGM PORT	1-3N	Mandatory
	SECONDARY AUTH URL	1-20X	Mandatory
	SECONDARY AUTH PORT	1-5N	Mandatory
	SECONDARY SETTLE URL	128X	Mandatory
	SECONDARY SETTLE PORT	1-5N	Mandatory
	SECONDARY HGM URL	128X	Mandatory
	SECONDARY HGM PORT	1-3N	Mandatory
	HGM EOD URL	128X	Mandatory
	PRIMARY ATTEMPTS	1N	Mandatory
	SECONDARY ATTEMPTS	1N	Mandatory

	HOST TYPE	1N	Mandatory
	VER NUM	1-4N	Mandatory
	SOAP URL	1-32X://X/X/X/X	Mandatory
	GATEWAY URL	1-32X://X	Mandatory
	PRIMARY WS URL	1-32 /X.X/X.X	Mandatory
	PORTICO PRIMARY URL	1-32X.X.X.X	Mandatory
	PORTICO PRIMARY PORT	1-3N	Mandatory
	PORTICO SECONDARY PORT	1-3N	Mandatory
DISPLAY/PROMPT TYPE PARAMETERS	IDLE TIMEOUT	1-2N	Mandatory
	KEY BEEP	B	Mandatory
	RESULT BEEP	B	Mandatory
	BEEP VOLUME	1-3N	Mandatory
	MULTI-APP TIMEOUT	B	Mandatory
	TABS	B	Mandatory
	BANNER TEXT 1	0-21X	Mandatory
	BANNER TEXT 2	0-21X	Mandatory
	LANE OPEN TEXT	0-21X	Mandatory
	LANE CLOSED TEXT	0-21X	Mandatory
DOWNLOAD TYPE	DOWNLOAD SOFTWARE ID	1-20X	Mandatory

PARAMETERS	DOWNLOAD TERMINAL ID	1-8X	Mandatory
	DOWNLOAD HOST URL	1-128X	Mandatory
	DOWNLOAD HOST PORT	1-4N	Mandatory
	PERFORM HEARTBEAT	B	Mandatory
	HEARTBEAT ERRORS	B	Mandatory
	HEARTBEAT SKIP DAYS	1N	Mandatory
	HEARTBEAT SKIP COMM	1N	Mandatory
	NFC FIRMWARE TID	1-8X	Mandatory
MERCHANT TYPE PARAMETERS	ACQUIRER BIN	1-6N	Mandatory
	AGENT BANK NUMBER	1-6N	Mandatory
	INDUSTRY MODE	1N	Mandatory
	DEVICE MODE	1N	Mandatory
	CHAIN NUMBER	1-6N	Mandatory
	CURRENCY CODE	1-3N	Mandatory
	FCS IDENTIFIER	1-6N	Mandatory
	HGM GIFT DOMAIN	1-32X	Mandatory
	HGM REWARDS DOMAIN	1-32X	Mandatory
	HGM PROFILE ID	1-32X	Mandatory
	HGM SELLER ID	1-32X	Mandatory

	MERCHANT ABA #	0-9N	Mandatory
	MERCHANT CITY	1-32X	Mandatory
	MERCHANT STATE	1-32X	Mandatory
	MERCHANT ZIP CODE	1-5N	Mandatory
	MERCH CATEGORY CODE	1-4N	Mandatory
	MERCHANT LOCATION #	1-5N	Mandatory
	MERCHANT NUMBER	1-12N	Mandatory
	MERCHANT SETTLE AGENT	1-5N	Mandatory
	PIN PAD TYPE	1N	Mandatory
	POS TYPE	1N	Mandatory
	PIN BYPASS ALLOWED	B	Mandatory
	NFC READER TYPE	1N	Mandatory
	STORE NUMBER	1-4N	Mandatory
	TERMINAL ID	1-8N	Mandatory
	TERMINAL NUMBER	1-4N	Mandatory
	TIME ZONE DIFF	1-4N	Mandatory
	FORCE QPS PIN	B	Mandatory
	STANDBY DELAY	1-3N	Mandatory
NETWORK TYPE	IP ADDRESS ASSIGNMENT	1N	Mandatory

PARAMETERS	IP ADDRESS	1-3N.N.N.N	Mandatory
	SUBNET MASK	1-3N.N.N.N	Mandatory
	DEFAULT GATEWAY	1-3N.N.N.N	Mandatory
	DNS SERVER 1	1-3N.N.N.N	Mandatory
	DNS SERVER 2	1-3N.N.N.N	Mandatory
	SIP LISTENING PORT	1-5N	Mandatory
TRANSACTION TYPE PARAMETERS	AUTO EOD PROC	B	Mandatory
	EOD PROC TIME	1-6N	Mandatory
	AUTO EOD RETRY MAX	1N	Mandatory
	BATCH NUMBER	3N	Mandatory
	CASHBACK SUPPORT	B	Mandatory
	EMV ENABLED	B	Mandatory
	EMV BEEP ENABLED	B	Mandatory
	EMV DIAGNOSTICS	B	Mandatory
	PDL DIAGNOSTICS	B	Mandatory
	GIFT ALLOWED	B	Mandatory
	PMT SELECT THRESHOLD	N	Mandatory
	SEND NOTIFICATION	B	Mandatory
	SAF MODE	1N	Mandatory



SETTLE ALLOW VOIDS	B	Mandatory
TIP SUPPORT	B	Mandatory
ALLOW TIP ASSIST	B	Mandatory
SPLIT TIP ENABLED	B	Mandatory
TIP ASSISTANCE 1	1-4N	Mandatory
TIP ASSISTANCE 2	1-4N	Mandatory
TIP ASSISTANCE 3	1-4N	Mandatory
WANT TO TIP PROMPT	B	Mandatory
WHITELIST ENABLED	B	Mandatory
ALLOW CASHBACK ASSIST	B	Mandatory
CASHBACK ASSISTANCE 1	1-4N	Mandatory
CASHBACK ASSISTANCE 2	1-4N	Mandatory
CASHBACK ASSISTANCE 3	1-4N	Mandatory

Every <Record> in a response will have the following characteristics:

- A similar XML heading
- Table category followed by 30 or less <Field> elements or
- 30 or less <Field> elements with no TableCategory.

Essentially the presence of TableCategory as a first element in the response record indicates the beginning of a new category of elements and the table category descriptor gives a very short description of the category.

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
```

```

<SIPId>16322SC81188236</SIPId>
<DeviceId>6225529</DeviceId>
<RequestId>10042</RequestId>
<Response>GetParameterReport</Response>
<ResponseId>10042</ResponseId>
<MultipleMessage>0</MultipleMessage>
<Result>0</Result>
<ResultText>Success</ResultText>
<Record>
  <TableCategory>CARD TYPE PARAMETERS</TableCategory>
  <Field>
    <Key>BEGINNING BIN</Key>
    <Value>4000000000</Value>
  </Field>
  <Field>
    <Key>ENDING BIN</Key>
    <Value>4999999999</Value>
  </Field>
  <Field>
    <Key>ENABLED</Key>
    <Value>ON</Value>
  </Field>
  <Field>
    <Key>LONG CARD NAME</Key>
    <Value>VISA</Value>
  </Field>
  <Field>
    <Key>SHORT CARD NAME</Key>
    <Value>VI</Value>
  </Field>
  <Field>
    <Key>CARD TYPE</Key>
    <Value>1</Value>
  </Field>
  ...
</Record>
</SIP>
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>10042</RequestId>
  <Response>GetParameterReport</Response>
  <ResponseId>10042</ResponseId>
  <MultipleMessage>1</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <Record>

```

```

<TableCategory>COMMUNICATION TYPE PARAMETERS</TableCategory>
<Field>
  <Key>PRIMARY AUTH URL</Key>
  <Value>test.txns.secureexchange.net</Value>
</Field>
<Field>
  <Key>PRIMARY AUTH PORT</Key>
  <Value>12345</Value>
</Field>
<Field>
  <Key>PRIMARY SETTLE URL</Key>
  <Value>test.txns.secureexchange.net</Value>
</Field>
<Field>
  <Key>PRIMARY SETTLE PORT</Key>
  <Value>12346</Value>
</Field>
<Field>
  <Key>PRIMARY HGM URL</Key>
  <Value>ctp.test.chockstone.com</Value>
</Field>
<Field>
  <Key>PRIMARY HGM PORT</Key>
  <Value>443</Value>
</Field>
<Field>
  <Key>SECONDARY AUTH URL</Key>
  <Value>test.txns.secureexchange.net</Value>
</Field>
  ...
</Record>
</SIP>

```

### 5.2.10. GetSAFReport Command

This command will return the Store and Forward (SAF) transaction details (one record at a time) from the SIP device to the POS.

HPA maintains a record of all SAF transactions processed within a single batch. Once the End of Day process is run, the SAF records will be available on the End of Day report.

**NOTE:** Pending SAF transactions that could not be uploaded before the batch closed will be stored and uploaded on the next batch.

This report will contain:

- Discarded SAFs
- Pending SAFs

- Approved SAFs
- Partially Approved SAFs
- Declined SAFs
- Void SAFs (Approved, Declined and Pending)

#### 5.2.10.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>GetSAFReport</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<FieldCount>	1-2N	Optional	See <a href="#">&lt;FieldCount&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.10.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>GetSAFReport</Request>
  <RequestId>100483</RequestId>
</SIP>

```

#### 5.2.10.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>

<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>GetSAFReport</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	1-10N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
<TableCategory>	See <a href="#">Record Data</a>	Conditional If new category of elements begin	See <a href="#">&lt;TableCategory&gt;</a>
<Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>
<Key>	See <a href="#">Record Data</a>	Mandatory	See <a href="#">&lt;Key&gt;</a>
<Value>	See <a href="#">Record Data</a>	Mandatory	See <a href="#">&lt;Value&gt;</a>
</Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>
...	--	--	<Field>, <Key>, <Value>, and </Field> elements repeat as specified for each Record/TableCategory per <a href="#">Record Data</a>
</Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.10.4. Record Data

<TableCategory>	<Key>	<Value>	Usage
APPROVED SAF SUMMARY	Count	1-4N	Mandatory

PENDING SAF SUMMARY DECLINED SAF SUMMARY OFFLINE APPROVED SAF SUMMARY PARTIALLY APPROVED SAF SUMMARY APPROVED SAF VOID SUMMARY PENDING SAF VOID SUMMARY DECLINED SAF VOID SUMMARY	Amount	1-7N	Conditional If not voided or partially approved
	Total Amount	1-7N	Conditional If partially approved
	Authorized Amount	1-7N	Conditional If partially approved
	Balance Due Amount	1-7N	Conditional If partially approved
Individual SAF Transaction e.g. PENDING SAF #1 RECORD	Responseld	1-10N	Mandatory
	TransactionId	1-10N	Mandatory
	OrigTransactionId	1-10N	Conditional If voided, TipAdjust, TransactionAdjust, Refund with Original TransactionId, CreditAdditionalAuth and CreditAuthComplete
	MaskedPAN	1-19X	Conditional If not voided or not token sale
	CardType	1-32X	Conditional If not voided or token sale is sent online
	CardAcquisition	1-6X	Conditional

		If not voided
HostTimeOut	B	Conditional If not voided
BaseAmount	1-7N	Conditional If not voided
TaxAmount	1-7N	Conditional If not voided
TipAmount	1-6N	Conditional If not voided
RequestAmount	1-7N	Conditional If not voided

#### 5.2.10.5. Response Example

The response will contain a summary showing the number of transactions (Count) and the total amount in those transactions (Amount) for approved, pending, declined, and partially approved and void (Approved, Pending and Declined) SAF transactions, respectively. This summary will constitute one message. This message will be followed by detailed transaction messages. The number of detailed messages will be equal to the sum of all SAF transactions.

After sending the summary records for ALL SAF TRANSACTIONS the SIP device will send a transaction detail record for each SAF transaction.

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100488</RequestId>
  <Response>GetSAFReport</Response>
  <ResponseId>100488</ResponseId>
  <MultipleMessage>1</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <Record>
    <TableCategory>APPROVED SAF SUMMARY</TableCategory>
    <Field>
      <Key>Count</Key>
      <Value>0</Value>
    </Field>
  </Record>

```

```

    <Field>
      <Key>Amount</Key>
      <Value>0</Value>
    </Field>
    ...
  </Record>
</SIP>

```

### 5.2.11. LaneClose Command

This command will transition the SIP device to “LANE CLOSE” state.

#### 5.2.11.1. Request schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>LaneClose</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.11.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>LaneClose</Request>
  <RequestId>10045</RequestId>
</SIP>

```

#### 5.2.11.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>



<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>LaneClose</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	1-10N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.11.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>10045</RequestId>
  <Response>LaneClose</Response>
  <ResponseId>10045</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
</SIP>

```

### 5.2.12. LaneOpen Command

This command will transition the SIP device to “LANE OPEN” state.

#### 5.2.12.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>

<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>LaneOpen</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.2.12.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>LaneOpen</Request>
  <RequestId>10046</RequestId>
</SIP>

```

### 5.2.12.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>LaneOpen</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	1-10N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>

</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
--------	----	-----------	---------------------------------

#### 5.2.12.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>10046</RequestId>
  <Response>LaneOpen</Response>
  <ResponseId>10046</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
</SIP>

```

### 5.2.13. ManagerMenu Command

This command will display HPA's manager menu on the SIP device. The idea is to keep the manager menu hidden from consumers/users and only display when the POS needs it. A Manager password is prompted on the SIP device. The HPA POS listener is not active (not accepting commands) while in the Manager function submenus.

Pressing the CANCEL key exits the Manager Menu and returns the SIP device to the Lane Closed state. The Response is sent when the Manager Menu exits.

#### 5.2.13.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>ManagerMenu</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.2.13.2. Request Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>ManagerMenu</Request>
  <RequestId>1004108</RequestId>
</SIP>
```

### 5.2.13.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>ManagerMenu</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	1-10N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.2.13.4. Response Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004108</RequestId>
  <Response>ManagerMenu</Response>
  <ResponseId>1004108</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
```

```

    <ResultText>Success</ResultText>
  </SIP>

```

## 5.2.14. Reboot Command

This command will reboot the SIP device.

### 5.2.14.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>Reboot</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.2.14.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>Reboot</Request>
  <RequestId>100423</RequestId>
</SIP>

```

### 5.2.14.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>

<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>Reboot</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	1-10N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.14.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100423</RequestId>
  <Response>Reboot</Response>
  <ResponseId>100423</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
</SIP>

```

#### 5.2.15. Reset Command

This command is used for two purposes: it is used to terminate a previously issued command such as a Sale transaction, and it is used to return the terminal to the idle state. The idle state can be “Lane Opened” state or a “Lane Closed” state.

Note that the Reset command must be sent after every administrative command with the exception of LaneOpen, LaneClose, SendFile, and Download.

It is important to understand that financial transaction result text such as APPROVED, DECLINED, or UNABLE TO PROCESS does not time out but is displayed until the POS sends a Reset command to clear the display and return the terminal to the idle state. The POS controls how long the transaction result text is displayed by the amount of time it waits after receiving the transaction response message before sending the Reset command.

During a financial transaction the POS may send a Reset command to cancel the transaction. If the Reset is successful (i.e. ResultText element is SUCCESS) then the terminal will cancel the transaction, display TRANSACTION CANCELED, send the Reset response followed by the transaction response message. The financial response message will have the ResultText element set to TRANSACTION CANCELED BY CLERK. The TRANSACTION CANCELED will continue to be displayed until the POS sends a Reset command to return the terminal to the idle state. Note that the flow is similar to normal financial transactions in that the POS sends a Reset command after receiving the transaction response message to clear the result text and return the terminal to the idle state.

To be clear, in the above scenario in which a Reset is used to cancel a Sale transaction there are two Resets sent by the POS. The first Reset cancels the transaction and is sent before the Sale response is received. The second Reset is sent after the Sale response is received and is used to clear the display and return the terminal to the idle state.

All other administrative commands require a Reset command following the command response. Failure to send a Reset command after the response is received for these commands will result in a SIP DEVICE BUSY error response on the next command.

#### 5.2.15.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>Reset</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.15.2. Request Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>Reset</Request>
  <RequestId>10047</RequestId>
</SIP>
```

## 5.2.15.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>Reset</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	1-10N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

## 5.2.15.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>10047</RequestId>
  <Response>Reset</Response>
  <ResponseId>10047</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
</SIP>

```



## 5.2.16. SendFile Command

The Send File command is used to send a file to HPA. A typical use case is to send merchant specific Logo and Banner image files. Refer to the User Interface section in this document for more details about image files.

- HPA will return an error if there is insufficient memory on the SIP device to store a file of size <FileSize> bytes as specified in the initial FileName request, or if <FileSize> is greater than 1MB.
- The maximum number of hexadecimal ASCII characters that can be included in the <FileData> element of each subsequent FileData request is specified in the initial FileName response in the <MaxDataSize> element.
- After the initial FileName request/response, the POS should continuously send subsequent FileData requests until all the file data has been transmitted to HPA.
- HPA will not send the FileData response until <FileSize> bytes have been received, or an error occurs.

**NOTE:** The maximum number of hexadecimal ASCII characters that can be included in the <FileData> element is 5120 bytes.

### 5.2.16.1. Supported Files

File Name	Pixel Dimensions (W x H)	Purpose
BANNER320.JPG	320 x 40 (Lane/3000)	Displayed at the top of the SIP device screen at all times during POS driven activities. It is not shown when doing HPA driven activities such as auto EOD processing.
BANNER480.JPG	480 x 60 (Lane/5000)	
BKG320.JPG	320 x 240 (Lane/3000)	Displayed at the background of each transaction screen. It is not shown at idle screen.
BKG480.JPG	480 x 320 (Lane/5000)	
LOGO320.JPG	320 x 240 (Lane/3000)	Displayed when the SIP device is in an idle state. The SIP device boots up into an idle state. Every command from the POS puts SIP device in an active state, and it returns to an idle state by a Reset command.
LOGO480.JPG	480 x 320 (Lane/5000)	

**NOTE:** File names are case sensitive in SendFile command.

**NOTE:** SendFile supports only .jpg/.JPG and .wgu/.WGU file formats.

## 5.2.16.2. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>SendFile</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<FileName>	1-14X	Conditional If initial request.	See <a href="#">&lt;FileName&gt;</a>
<FileSize>	1-7N	Conditional If initial request.	See <a href="#">&lt;FileSize&gt;</a>
<FileData>	var.	Conditional If subsequent request.	See <a href="#">&lt;FileData&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

## 5.2.16.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>SendFile</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>

<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<MaxDataSize>	1-7N	Conditional If initial response.	See <a href="#">&lt;MaxDataSize&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.16.4. Initial FileName Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>SendFile</Request>
  <RequestId>1004177</RequestId>
  <FileName>BANNER.JPG</FileName>
  <FileSize>21954</FileSize>
  <MultipleMessage>1</MultipleMessage>
</SIP>

```

#### 5.2.16.5. Initial FileName Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004177</RequestId>
  <Response>SendFile</Response>
  <ResponseId>1004177</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <MaxDataSize>5120</MaxDataSize>
</SIP>

```

#### 5.2.16.6. Subsequent FileData Request Examples

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>SendFile</Request>
  <RequestId>1004178</RequestId>
  <FileData>FFD8FFE000104A46494600010101012C012C0000FFE1322D687474703A2F2F6E732
E61646F62652E636F6D2F7861702F312E302F003C3F787061636B657420626567696E3D22EFBB
BF222069643D2257354D304D7043656869487A7265537A4E54637A6B633964223F3E0D0A3C783
A786D706D65746120786D6C6E733A783D2261646F62653A6E733A6D6574612F2220783A786D70
746B3D2241646F626520584D5020436F726520352E302D633036302036312E3133343737372C2

```

[illegible]

### 5.2.16.7. FileData Response Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004177</RequestId>
  <Response>SendFile</Response>
  <ResponseId>1004177</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <MaxDataSize>5120</MaxDataSize>
</SIP>
```

### 5.2.16.8. Error Response Example

An error response can be generated at any of the requests above.

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004222</RequestId>
  <Response>SendFile</Response>
  <ResponseId>1004222</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>2955</Result>
  <ResultText>INVALID FILE NAME</ResultText>
</SIP>
```

### 5.2.17. SendSAF Command

This command will attempt to upload any pending Store and Forward transactions to the host for authorization.

- The SAF Report is always returned in the response.
- The SAF Report will contain any:
  - Approved SAFs
  - Partially Approved SAFs
  - Declined SAFs
  - Pending SAFs
  - Voided SAFs (Approved, Declined and Pending)

**NOTE:** SendSAF will not process any Provisional or Discarded SAF transactions from SAF Batch.

#### 5.2.17.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>SendSAF</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>

</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
--------	----	-----------	---------------------------------

### 5.2.17.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>SendSAF</Request>
  <RequestId>100494</RequestId>
</SIP>

```

### 5.2.17.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Conditional If returned by host	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>SendSAF</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<Responseld>	4-16N	Mandatory	See <a href="#">&lt;Responseld&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
<TableCategory>	See Record Data	Conditional If new category of elements begin	See <a href="#">&lt;TableCategory&gt;</a>
<Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>
<Key>	See Record Data	Mandatory	See <a href="#">&lt;Key&gt;</a>

<Value>	See Record Data	Mandatory	See <a href="#">&lt;Value&gt;</a>
</Field>	--	Mandatory	See <a href="#">&lt;Field&gt;</a>
...	--	--	<Field>, <Key>, <Value>, and </Field> elements repeat as specified for each Record/TableCategory per Record Data
</Record>	--	Mandatory	See <a href="#">&lt;Record&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.17.4. Record Data

<TableCategory>	<Key>	<Value>	Usage
APPROVED SAF SUMMARY PENDING SAF SUMMARY PROVISIONAL SAF SUMMARY DISCARDED SAF SUMMARY DECLINED SAF SUMMARY OFFLINE APPROVED SAF SUMMARY APPROVED SAF VOID SUMMARY PENDING SAF VOID SUMMARY PROVISIONAL SAF VOID SUMMARY DISCARDED SAF VOID SUMMARY DECLINED SAF VOID SUMMARY PARTIALLY APPROVED SAF SUMMARY	Count	1-4N	Mandatory
	Amount	1-7N	Conditional If not voided or partially approved
	Total Amount	1-7N	Conditional If partially approved
	Authorized Amount	1-7N	Conditional If partially approved
	Balance Due Amount	1-7N	Conditional If partially approved
Individual Approved SAF Record e.g. APPROVED SAF #1 RECORD	Responseld	1-10N	Mandatory
	TransactionId	1-10N	Mandatory
	OrigTransactionId	1-10N	Conditional If Void, TipAdjust, TransactionAdjust, Refund, CreditAdditionalAuth

		or CreditAuthComplete with Original TransactionId
TransactionTime	12N	Mandatory
TransactionType	4-6X	Mandatory
MaskedPAN	1-19X	Mandatory
CardType	1-32X	Mandatory
CardAcquisition	1-6X	Mandatory
ApprovalCode	6N	Mandatory
ResponseCode	2N	Mandatory
ResponseText	16X	Mandatory
HostTimeOut	B	Mandatory

#### 5.2.17.5. Response Example

The SendSAF response message begins with a summary record showing the number of approved SAF transactions:

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100486</RequestId>
  <Response>SendSAF</Response>
  <ResponseId>1024810318</ResponseId>
  <MultipleMessage>1</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <Record>
    <TableCategory>APPROVED SAF SUMMARY</TableCategory>
    <Field>
      <Key>Count</Key>
    
```



```

        <Value>2</Value>
    </Field>
    <Field>
        <Key>Amount</Key>
        <Value>2198</Value>
    </Field>
</Record>
</SIP>

```

### 5.2.18. SetClock Command

This command sets the date and time on the SIP device.

**NOTE:** The date valid range is from 01/01/1900 to 12/31/2100 but entering an invalid date for the location may have adverse consequences for transactions.

#### 5.2.18.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>SetClock</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Time>	14N	Mandatory	See <a href="#">&lt;Time&gt;</a>
</SIP>		Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.18.2. Request Example

```

<SIP>
    <Version>1.0</Version>
    <ECRId>1004</ECRId>
    <Request>SetClock</Request>
    <RequestId>100417</RequestId>
    <Time>20170913171256</Time>
</SIP>

```

#### 5.2.18.3. Response Schema

XML Element	Value	Usage	Description
-------------	-------	-------	-------------

<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>SetClock</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	1-10N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<DateTime>	14N	Optional	See <a href="#">&lt;DateTime&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.18.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100417</RequestId>
  <Response>SetClock</Response>
  <ResponseId>100417</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <DateTime>20170913171256</DateTime>
</SIP>

```

### 5.2.19. SetParameter Command

This command is used to set application parameters used by SIP. The request contains the FieldCount number of Key-Value pairs sent in the request. There is only one FieldCount element per request and it can range from 1 to 30. The Key element is the name of the parameter and must exactly match the name used in the parameter table shown in Communication Parameters through Miscellaneous Parameters. The Value is what the parameter will be set to and must be of the same type as shown in the table.

**NOTE:** We **strongly** recommend that any parameter changes are managed through normal support channels and updated via a partial download for the following reasons:

- Any parameters updated locally by the POS may be reverted on subsequent downloads if they are not also set at HUDS.
- Update to some Communication parameters, such as POSLNKTYP, will immediately cause the POS to HPA communication not to work if the communication type is not updated accordingly on the POS side.

#### 5.2.19.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>SetParameter</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<FieldCount>	1-2N	Mandatory	See <a href="#">&lt;FieldCount&gt;</a>
<Key>	1-32X	Mandatory	See <a href="#">&lt;Key&gt;</a>
<Value>	Depends on parameter	Mandatory	See <a href="#">&lt;Value&gt;</a>
</SIP>		Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.2.19.2. Request Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>SetParameter</Request>
  <RequestId>100411</RequestId>
```

```

    <FieldCount>1</FieldCount>
    <Key>STORMD</Key>
    <Value>3</Value>
</SIP>

```

### 5.2.19.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Conditional If returned by host	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>SetParameter</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<Responseld>	1-10N	Mandatory	See <a href="#">&lt;Responseld&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.2.19.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100411</RequestId>
  <Response>SetParameter</Response>

```

```

<ResponseId>100411</ResponseId>
<MultipleMessage>0</MultipleMessage>
<Result>0</Result>
<ResultText>Success</ResultText>
</SIP>

```

## 5.3. Transaction Commands

- Transaction commands work only in a “Lane Open” state.
- Transaction commands will go through the screen flows and will stay at the last screen without a time out. A Reset command is expected to go to “Lane Open” state.
- If used in a “Lane Closed” state, SIP device will respond with a “CANNOT PROCESS IN A LANE CLOSE STATE” error response.
- While processing a Transaction command, the only command that may be sent from the POS is the Reset command, all other commands will receive a “SIP DEVICE BUSY” error response.
- A Transaction function can be cancelled and returned to the “Lane Open” state either by a Reset command, by pressing CANCEL on the SIP device, or a Time out on a screen that is prompting for user input.

**DISCLAIMER:** The Request and Response messages below are EXAMPLES ONLY, and may not contain all possible XML elements that can be sent to or received from HPA. Refer to the schema for a complete list of XML elements that may be included.

### 5.3.1. AddValue Command

This command instructs HPA to add value to a Gift Card.

**NOTE:** If the WHITELIST parameter is enabled, HPA will check the card’s PAN against a whitelist , if the PAN matches a whitelist BIN then HPA will not run the AddValue command but instead return the track data to the POS.

#### 5.3.1.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>

<Request>	<b>AddValue</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<TotalAmount>	1-7N	Mandatory	See <a href="#">&lt;TotalAmount&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.1.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>AddValue</Request>
  <RequestId>100428</RequestId>
  <TotalAmount>200</TotalAmount>
</SIP>

```

### 5.3.1.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Conditional If returned by host	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>Addvalue</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<Responseld>	4-16N	Mandatory	See <a href="#">&lt;Responseld&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<TransactionTime>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>
<GatewayRspCode>	1-4N	Conditional	See

		If returned by host	<a href="#">&lt;GatewayRspCode&gt;</a>
<GatewayRspMsg>	1-34X	Conditional If returned by host	See <a href="#">&lt;GatewayRspMsg&gt;</a>
<ResponseCode>	2N	Conditional if Host response received	See <a href="#">&lt;ResponseCode&gt;</a>
<ResponseText>	1-200X	Conditional if Host response received	See <a href="#">&lt;ResponseText&gt;</a>
<ApprovalCode>	6N	Conditional if Approved	See <a href="#">&lt;ApprovalCode&gt;</a>
<CardholderName>	28X	Conditional if read from the card	See <a href="#">&lt;CardholderName&gt;</a>
<CardType>	16X	Conditional If Card acquired	See <a href="#">&lt;CardType&gt;</a>
<CardGroup>	1-6X	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
<CardAcquisition>	7X	Conditional If Card acquired	See <a href="#">&lt;CardAcquisition&gt;</a>
<MaskedPAN>	16N or 19N	Conditional If Card acquired	See <a href="#">&lt;MaskedPAN&gt;</a>
<SignatureLine>	1N	Conditional if Approved	See <a href="#">&lt;SignatureLine&gt;</a>
<PinVerified>	1N	Conditional if Approved	See <a href="#">&lt;PinVerified&gt;</a>
<AuthorizedAmount>	9N	Mandatory	See <a href="#">&lt;AuthorizedAmount&gt;</a>
<BalanceAmount>	9N	Conditional if Approved	See <a href="#">&lt;BalanceAmount&gt;</a>
<ClearPAN>	19N	If Whitelist Gift card	See <a href="#">&lt;ClearPAN&gt;</a>
<TrackNumber>	1N	If Whitelist Gift card	See <a href="#">&lt;TrackNumber&gt;</a>
<TrackData>	128X	If Whitelist Gift card	See <a href="#">&lt;TrackData&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.3.1.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100428</RequestId>
  <Response>AddValue</Response>
  <ResponseId>1024697427</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>091117070556</TransactionTime>
  <GatewayRspCode>0</GatewayRspCode>
  <GatewayRspMsg>Success</GatewayRspMsg>
  <ResponseCode>0</ResponseCode>
  <ResponseText>Success</ResponseText>
  <ApprovalCode>091107</ApprovalCode>
  <CardType>GIFT/REWARDS</CardType>
  <CardGroup>GIFT</CardGroup>
  <CardAcquisition>SWIPE</CardAcquisition>
  <MaskedPAN>*****0098</MaskedPAN>
  <SignatureLine>0</SignatureLine>
  <PinVerified>0</PinVerified>
  <AuthorizedAmount>200</AuthorizedAmount>
  <BalanceAmount>1220</BalanceAmount>
</SIP>

```

#### 5.3.1.5. Gift Card Whitelist Add Value

If a Gift Card matching the whitelist is used for the Add Value command then the SIP Device will respond with a whitelist response containing the track data. The POS will then run the transaction and send a Display Message command to the SIP Device as shown below.

##### 5.3.1.5.1. Gift Card Add Value Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>AddValue</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>



<TotalAmount>	1-7N	Mandatory	See <a href="#">&lt;TotalAmount&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.3.1.5.1.1. Request Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>AddValue</Request>
  <RequestId>100442</RequestId>
  <TotalAmount>1200</TotalAmount>
</SIP>
```

#### 5.3.1.5.1.2. Response Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <SIPId>15293SC80802518</SIPId>
  <DeviceId>6194404</DeviceId>
  <RequestId>10046</RequestId>
  <Response>AddValue</Response>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>022616160849</TransactionTime>
  <CardAcquisition>SWIPE</CardAcquisition>
  <ClearPAN>6006496689000000001</ClearPAN>
  <TrackNumber>2</TrackNumber>
  <TrackData>6006496689000000001=25121019888877776</TrackData>
</SIP>
```

## 5.3.2. BalanceInquiry Command

This command instructs HPA to perform a Balance Inquiry.

**NOTE:** If performed for a Gift and the card used for the balance inquiry transaction matches the whitelist, then a whitelist balance inquiry transaction is performed. In this case HPA returns cleartext PAN and track data, the normal host response elements are not returned.

#### 5.3.2.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>

<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>BalanceInquiry</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<CardGroup>	EBT/GIFT	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.2.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>BalanceInquiry</Request>
  <RequestId>100497</RequestId>
  <CardGroup>EBT</CardGroup>
</SIP>

```

### 5.3.2.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Conditional If returned by host	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>BalanceInquiry</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<TransactionTime>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>

<GatewayRspCode>	1-4N	Conditional If returned by host	See <a href="#">&lt;GatewayRspCode&gt;</a>
<GatewayRspMsg>	1-34X	Conditional If returned by host	See <a href="#">&lt;GatewayRspMsg&gt;</a>
<ResponseCode>	2N	Conditional if Host response received	See <a href="#">&lt;ResponseCode&gt;</a>
<ResponseText>	1-200X	Conditional if Host response received	See <a href="#">&lt;ResponseText&gt;</a>
<CardholderName>	28X	Conditional if read from the card	See <a href="#">&lt;CardholderName&gt;</a>
<CardType>	16X	Conditional If Card acquired	See <a href="#">&lt;CardType&gt;</a>
<EBTType>	12X	Conditional If the transaction is EBT	See <a href="#">&lt;EBTType&gt;</a>
<CardGroup>	1-6X	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
<CardAcquisition>	7X	Conditional If Card acquired	See <a href="#">&lt;CardAcquisition&gt;</a>
<MaskedPAN>	16N or 19N	Conditional If Card acquired	See <a href="#">&lt;MaskedPAN&gt;</a>
<PinVerified>	1N	Conditional if Approved	See <a href="#">&lt;PinVerified&gt;</a>
<AvailableBalance>	9N	If balance returned by host	See <a href="#">&lt;AvailableBalance&gt;</a>
<ClearPAN>	19N	If Whitelist Gift card	See <a href="#">&lt;ClearPAN&gt;</a>
<TrackNumber>	1N	If Whitelist Gift card	See <a href="#">&lt;TrackNumber&gt;</a>
<TrackData>	128X	If Whitelist Gift card	See <a href="#">&lt;TrackData&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.3.2.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>

```

```

<SIPId>16322SC81188236</SIPId>
<DeviceId>6225529</DeviceId>
<RequestId>1004103</RequestId>
<Response>BalanceInquiry</Response>
<ResponseId>1024691856</ResponseId>
<MultipleMessage>0</MultipleMessage>
<Result>0</Result>
<ResultText>Success</ResultText>
<TransactionTime>091117093630</TransactionTime>
<GatewayRspCode>0</GatewayRspCode>
<GatewayRspMsg>Success</GatewayRspMsg>
<ResponseCode>00</ResponseCode>
<ResponseText>APPROVAL</ResponseText>
<CardType>EBT</CardType>
<EBTType>CashBenefits</EBTType>
<CardGroup>EBT</CardGroup>
<CardAcquisition>SWIPE</CardAcquisition>
<MaskedPAN>*****4111</MaskedPAN>
<PinVerified>1</PinVerified>
<AvailableBalance>218040</AvailableBalance>
</SIP>

```

### 5.3.3. CardVerify Command

This command initiates a credit card verification transaction.

- The Card Verify transaction is used to verify that the card account is valid.
- The application sends a CreditAccountVerify message to Portico to validate the card.
- EMV cards are supported for Card Verify.
- For American Express cards the application will prompt for zip code.
- Card verify can be used to create a token for the card data, by including  
 <TokenRequest>1</TokenRequest> in the XML request to HPA

#### 5.3.3.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>

<Request>	<b>CardVerify</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<CardGroup>	<b>All</b> or <b>Credit</b>	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
<TokenRequest>	1N	Optional	See <a href="#">&lt;TokenRequest&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.3.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>CardVerify</Request>
  <RequestId>10043</RequestId>
  <CardGroup>All</CardGroup>
  <TokenRequest>1</TokenRequest>
</SIP>

```

### 5.3.3.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	n/a	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>CardVerify</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	1-10N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>

<TransactionTime>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>
<GatewayRspCode>	1-4N	Conditional If returned by gateway	See <a href="#">&lt;GatewayRspCode&gt;</a>
<GatewayRspMsg>	1-34X	Conditional If returned by gateway	See <a href="#">&lt;GatewayRspMsg&gt;</a>
<ResponseCode>	2N	Conditional If returned by host	See <a href="#">&lt;ResponseCode&gt;</a>
<ResponseText>	16X	Conditional If returned by host	See <a href="#">&lt;ResponseText&gt;</a>
<ApprovalCode>	6N	Conditional If approved	See <a href="#">&lt;ApprovalCode&gt;</a>
<ReferenceNumber>	4-16N	Conditional If approved	See <a href="#">&lt;ReferenceNumber&gt;</a>
<CardholderName>	28X	Conditional If read from card	See <a href="#">&lt;CardholderName&gt;</a>
<CardType>	16X	Conditional If card acquired	See <a href="#">&lt;CardType&gt;</a>
<CardGroup>	1-6X	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
<CardAcquisition>	7X	Conditional If card acquired	See <a href="#">&lt;CardAcquisition&gt;</a>
<MaskedPAN>	15-19N	Conditional If card acquired	See <a href="#">&lt;MaskedPAN&gt;</a>
<EMV_AID>	10-32X	Conditional If EMV transaction	See <a href="#">&lt;EMV_AID&gt;</a>
<EMV_ApplicationName>	32X	Conditional If EMV transaction	See <a href="#">&lt;EMV_ApplicationName&gt;</a>
<EMV_TVR>	4X	Conditional If EMV transaction	See <a href="#">&lt;EMV_TVR&gt;</a>
<EMV_TSI>	4X	Conditional If EMV transaction	See <a href="#">&lt;EMV_TSI&gt;</a>

<EMV_CryptogramType>	2X	Conditional If EMV transaction	See <a href="#">&lt;EMV_CryptogramType&gt;</a>
<EMV_Cryptogram>	16X	Conditional If EMV transaction	See <a href="#">&lt;EMV_Cryptogram&gt;</a>
<PinVerified>	1N	Conditional If approved	See <a href="#">&lt;PinVerified&gt;</a>
<TokenRspCode>	1-4N	Conditional If token requested	See <a href="#">&lt;TokenRspCode&gt;</a>
<TokenRspMsg>	1-34X	Conditional If token requested	See <a href="#">&lt;TokenRspMsg&gt;</a>
<TokenValue>	1-34X	Conditional If token requested	See <a href="#">&lt;TokenValue&gt;</a>
</SIP>		Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.3.3.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>10043</RequestId>
  <Response>CardVerify</Response>
  <ResponseId>1024688323</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>091117044750</TransactionTime>
  <GatewayRspCode>0</GatewayRspCode>
  <GatewayRspMsg>Success</GatewayRspMsg>
  <ResponseCode>85</ResponseCode>
  <ResponseText>CARD OK</ResponseText>
  <ApprovalCode>073689</ApprovalCode>
  <ReferenceNumber>725414052114</ReferenceNumber>
  <CardholderName>UAT USA/Test Card 07</CardholderName>
  <CardType>MASTERCARD</CardType>
  <CardGroup>CREDIT</CardGroup>
  <CardAcquisition>INSERT</CardAcquisition>
  <MaskedPAN>*****4111</MaskedPAN>
  <EMV_AID>A0000000041010</EMV_AID>
  <EMV_ApplicationName>MasterCard</EMV_ApplicationName>
  <EMV_TVR>0000208000</EMV_TVR>
  <EMV_TSI>E800</EMV_TSI>
  <EMV_CryptogramType>ARQC</EMV_CryptogramType>

```

```

<EMV_Cryptogram>2556438E26F15715</EMV_Cryptogram>
<PinVerified>0</PinVerified>
<TokenRspCode>0</TokenRspCode>
<TokenRspMsg>Success</TokenRspMsg>
<Tokenvalue>JP21fN08Ed4QA9WkA14C0016</Tokenvalue>
</SIP>

```

### 5.3.4. CreditAuth Command

The CreditAuth command is used to initiate a Pre-Auth transaction.

- The CreditAuth transaction is used as a pre-authorization to ensure that there is sufficient credit available on a card.
- EMV cards are supported for the Credit Auth transaction. If a communication failure occurs while sending the CreditAuth message then the reversal is stored as a piggyback and sent as a reversal with the next transaction.
- The transaction is not settled and is not included in the batch totals unless/until the pre-auth is completed using the CreditAuthComplete command.

#### 5.3.4.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>CreditAuth</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<TotalAmount>	1-7N	Mandatory	See <a href="#">&lt;TotalAmount&gt;</a>
<TokenValue>	1-34X	Optional	See <a href="#">&lt;TokenValue&gt;</a>
<InvoiceNbr>	1-25A	Optional	See <a href="#">&lt;InvoiceNbr&gt;</a>
<TokenRequest>	1N	Optional	See <a href="#">&lt;TokenRequest&gt;</a>
<SignaturePrompt>	1N	Optional	See <a href="#">&lt;SignaturePrompt&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>



### 5.3.4.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <Request>CreditAuth</Request>
  <RequestId>10040</RequestId>
  <TotalAmount>100</TotalAmount>
  <TokenValue>JP21fN08Ed4QA9WkA14C0016</TokenValue>
  <SignaturePrompt>0</SignaturePrompt>
</SIP>

```

### 5.3.4.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<Response>	<b>CreditAuth</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<TransactionTime>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<GatewayRspCode>	1-4N	Conditional If returned by gateway	See <a href="#">&lt;GatewayRspCode&gt;</a>
<GatewayRspMsg>	1-34X	Conditional If returned by gateway	See <a href="#">&lt;GatewayRspMsg&gt;</a>

<ResponseCode>	2N	Conditional If returned by host	See <a href="#">&lt;ResponseCode&gt;</a>
<ResponseText>	6N	Conditional If returned by host	See <a href="#">&lt;ResponseText&gt;</a>
<ApprovalCode>	6X	Conditional If returned by host	See <a href="#">&lt;ApprovalCode&gt;</a>
<ReferenceNumber>	4-16N	Conditional If returned by host	See <a href="#">&lt;ReferenceNumber&gt;</a>
<CardholderName>	28X	Conditional if read from the card	See <a href="#">&lt;CardholderName&gt;</a>
<CardType>	16X	Mandatory	See <a href="#">&lt;CardType&gt;</a>
<CardGroup>	1-6X	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
<CardAcquisition>	7X	Mandatory	See <a href="#">&lt;CardAcquisition&gt;</a>
<MaskedPAN>	19X	Mandatory	See <a href="#">&lt;MaskedPAN&gt;</a>
<SignatureLine>	1N	Mandatory	See <a href="#">&lt;SignatureLine&gt;</a>
<PinVerified>	1N	Mandatory	See <a href="#">&lt;PinVerified&gt;</a>
<TipAdjustAllowed>	1N	Mandatory	See <a href="#">&lt;TipAdjustAllowed&gt;</a>
<AVSResultText>	1-32X	Conditional if returned by host	See <a href="#">&lt;AVSResultText&gt;</a>
<CVVResultText>	1-32X	Conditional if returned by host	See <a href="#">&lt;CVVResultText&gt;</a>
<AuthorizedAmount>	1-9N	Mandatory	See <a href="#">&lt;AuthorizedAmount&gt;</a>
<TokenRspCode>	1-4N	Conditional If token requested	See <a href="#">&lt;TokenRspCode&gt;</a>
<TokenRspMsg>	1-34X	Conditional If token requested	See <a href="#">&lt;TokenRspMsg&gt;</a>
<TokenValue>	1-34X	Conditional If token requested	See <a href="#">&lt;TokenValue&gt;</a>

</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
--------	----	-----------	---------------------------------

#### 5.3.4.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <SIPIId>15292SC80802174</SIPIId>
  <DeviceId>5572626</DeviceId>
  <Response>CreditAuth</Response>
  <RequestId>10040</RequestId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>SUCCESS</ResultText>
  <TransactionTime>042417131417</TransactionTime>
  <ResponseId>1019630204</ResponseId>
  <GatewayRspCode>0</GatewayRspCode>
  <GatewayRspMsg>Success</GatewayRspMsg>
  <ResponseCode>00</ResponseCode>
  <ResponseText>APPROVAL</ResponseText>
  <ApprovalCode>068923</ApprovalCode>
  <ReferenceNumber>711419737702</ReferenceNumber>
  <CardholderName>AMEX TEST CARD</CardholderName>
  <CardType>AMERICAN EXPRESS</CardType>
  <CardGroup>CREDIT</CardGroup>
  <CardAcquisition>SWIPE</CardAcquisition>
  <MaskedPAN>*****1018</MaskedPAN>
  <SignatureLine>0</SignatureLine>
  <PinVerified>0</PinVerified>
  <TipAdjustAllowed>1</TipAdjustAllowed>
  <AuthorizedAmount>1122</AuthorizedAmount>
  <TokenRspCode>0</TokenRspCode>
  <TokenRspMsg>Success</TokenRspMsg>
  <TokenValue>JP21fN08Ed4QA9WkA14C0016</TokenValue>
</SIP>

```

**NOTE:** Token will not be generated for SAFed Credit Auth. So for SAFed Credit Auth, response will contain a dummy Token response with:

```

<TokenRspCode>99</TokenRspCode>
<TokenRspMsg>Could Not Generate Token Offline</TokenRspMsg>

```

#### 5.3.5. CreditAdditionalAuth Command

The CreditAdditionalAuth command is used to perform an additional preauthorization transaction in anticipation that the final preauth completion will be for an amount greater than the original preauthorization.

## 5.3.5.1. Request Schema

XML Element	Value	Usage	Descriptionrelease_HeartPOSv3.3o
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>CreditAdditionalAuth</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<TransactionId>	4-16N	Mandatory	See <a href="#">&lt;TransactionId&gt;</a>
<AdditionalAmount>	1-7N	Mandatory	See <AdditionalAmount>
<InvoiceNbr>	1-25A	Optional	See <a href="#">&lt;InvoiceNbr&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

## 5.3.5.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <RequestId>1004160</RequestId>
  <Request>CreditAdditionalAuth</Request>
  <TransactionId>1024844759</TransactionId>
  <AdditionalAmount>1150</AdditionalAmount>
</SIP>

```

## 5.3.5.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>

<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>CreditAdditionalAuth</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<TransactionTime>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>
<GatewayRspCode>	1-4N	Conditional If returned by gateway.	See <a href="#">&lt;GatewayRspCode&gt;</a>
<GatewayRspMsg>	1-34X	Conditional If returned by gateway.	See <a href="#">&lt;GatewayRspMsg&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.3.5.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004160</RequestId>
  <Response>CreditAdditionalAuth</Response>
  <ResponseId>1024844766</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>091417110139</TransactionTime>
  <GatewayRspCode>0</GatewayRspCode>
  <GatewayRspMsg>Success</GatewayRspMsg>
</SIP>

```

#### 5.3.6. CreditAuthComplete Command

The CreditAuthComplete command is used to complete the Pre-Auth transaction by instructing Portico to add the transaction to the batch for settlement.

**NOTE:** The transaction may also be edited if necessary, e.g. to specify a final settlement amount less than the original pre-authorized amount, to add or adjust a tip, etc.

### 5.3.6.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>CreditAuthComplete</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<TransactionId>	4-16N	Mandatory	See <a href="#">&lt;TransactionId&gt;</a>
<TotalAmount>	1-7N	Optional	See <a href="#">&lt;TotalAmount&gt;</a>
<TipAmount>	1-6N	Optional	See <a href="#">&lt;TipAmount&gt;</a>
<SignaturePrompt>	1N	Optional	See <a href="#">&lt;SignaturePrompt&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.6.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <RequestId>1004160</RequestId>
  <Request>CreditAuthComplete</Request>
  <TransactionId>1024844759</TransactionId>
  <TotalAmount>1150</TotalAmount>
  <TipAmount>250</TipAmount>
  <SignaturePrompt>0</SignaturePrompt>
</SIP>

```

### 5.3.6.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>

<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>CreditAuthComplete</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<TransactionTime>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>
<GatewayRspCode>	1-4N	Conditional If returned by gateway	See <a href="#">&lt;GatewayRspCode&gt;</a>
<GatewayRspMsg>	1-34X	Conditional If returned by gateway	See <a href="#">&lt;GatewayRspMsg&gt;</a>
<ResponseCode>	2N	Conditional If returned by host	See <a href="#">&lt;ResponseCode&gt;</a>
<ResponseText>	6X	Conditional If returned by host	See <a href="#">&lt;ResponseText&gt;</a>
<SignatureLine>	1N	Conditional If approved	See <a href="#">&lt;SignatureLine&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.3.6.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004160</RequestId>
  <Response>CreditAuthComplete</Response>
  <ResponseId>1024844766</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>091417110139</TransactionTime>
  <GatewayRspCode>0</GatewayRspCode>

```

```

<GatewayRspMsg>Success</GatewayRspMsg>
<ResponseCode>00</ResponseCode>
<ResponseText>APPROVAL</ResponseText>
<SignatureLine>0</SignatureLine>
</SIP>

```

### 5.3.7. GetCardData Command

This command is used to request card data for non-payment cards, such as manager cards. HeartPOS will prompt for card acquisition using swipe and will validate that the data on the card does not match bank card BIN ranges. If the card is swiped and it doesn't match a bank card format and BIN range, then HPA will return the track data using the <TrackNumber> and <TrackData> elements.

- The GetCardData command is used to get track data from specialty cards used for administrative purposes. For example, there may be a “manager” card used to login to the POS.
- No message is sent to Portico, this is a local operation.
- The application prompts for the card to be swiped. Only card swipe is supported.
- The application examines the track data, if the track data contains an account number that matches any known bank card, then the application displays CARD NOT ALLOWED and returns to the card acquisition screen after pressing a key.

**NOTE:** GetCardData is not intended to be used with payment cards, and we strongly recommend that this command not be used for financial transactions due to the fact that it intentionally returns clear track data. It is intended for administrative functions only. See Gift Card WhiteList Processing for obtaining track data for a third-party stored value provider.

#### 5.3.7.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>GetCardData</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>



### 5.3.7.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>GetCardData</Request>
  <RequestId>100424</RequestId>
</SIP>

```

### 5.3.7.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Conditional If returned by host.	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>GetCardData</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<TransactionTime>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>
<ClearPAN>	19N	If Whitelist Gift card	See <a href="#">&lt;ClearPAN&gt;</a>
<TrackNumber>	1N	If Whitelist Gift card	See <a href="#">&lt;TrackNumber&gt;</a>
<TrackData>	128X	If Whitelist Gift card	See <a href="#">&lt;TrackData&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.7.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <SIPId>[SIP ID]</SIPId>
  <DeviceId>[DEVICE ID]</DeviceId>
  <RequestId>[REQUEST ID]</RequestId>
  <Response>GetCardData </Response>
  <ResponseId>[RESPONSE ID]</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>[Status]</ResultText>
  <TransactionTime>082417110930</TransactionTime>
  <ClearPAN>6299290010000010</ClearPAN>
  <TrackNumber>1</TrackNumber>
  <TrackData>B6299290010000010^ONE PRINCETON TEST CARD
1^2512101180390000000000396</TrackData>
  <TrackNumber>2</TrackNumber>
  <TrackData>6299290010000010=25121011803939600000</TrackData>
</SIP>

```

### 5.3.8. LineItem Command

The POS may display information about the items being rung up by the clerk, such as a description, cost, and running total, on the SIP device by using the LineItem command. The command should be sent for each item that is rung up, along with optional running text if desired.

**NOTE:** This feature cannot be used in conjunction with the card acquisition on demand feature.

#### 5.3.8.1. Line Item Display

The middle portion of the SIP screen will be used to display line items.

- Up to 7 line items may be displayed at a time.
- If more than 7 items are rung up, the line items will scroll up with the most recent item being displayed at the bottom of the list.
- If running text is specified, only 5 items will be displayed at a time, with a blank line between the line items and running text. The running text will be bolded.

Heartland	
LINE ITEM #1	2.35
LINE ITEM #2	3.67
LINE ITEM #3	1.29
LINE ITEM #4	4.36

LINE ITEM #5	2.59
LINE ITEM #6	5.28
LINE ITEM #7	1.36

Heartland	
LINE ITEM #1	2.35
LINE ITEM #2	3.67
LINE ITEM #3	1.29
LINE ITEM #4	4.36
LINE ITEM #5	2.59
<b>TOTAL</b>	<b>14.26</b>

### 5.3.8.2. Subsequent Processing

The commands that are permitted to follow the Lineltem command are:

- Lineltem (next line item to display)
- Sale
- Refund
- Reset

If any other commands follow Lineltem, HPA will respond with a “SIP DEVICE BUSY” result.

### 5.3.8.3. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>Lineltem</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<LineltemTextLeft>	1-32X*	Mandatory	See <a href="#">&lt;LineltemTextLeft&gt;</a>
<LineltemTextRight>	1-32X*	Optional	See <a href="#">&lt;LineltemTextRight&gt;</a>
<LineltemRunningTextLeft>	1-32X*	Optional	See <a href="#">&lt;LineltemRunningTextLeft&gt;</a>
<LineltemRunningTextRight>	1-32X*	Optional	See

			<a href="#">&lt;LineItemRunningTextRight&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

\*The POS may send up to 70 characters of text in each of these XML elements, but currently only 32 total characters will be displayed on each line based on the font being used on the Lane/5000.

#### 5.3.8.4. Request Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>LineItem</Request>
  <RequestId>100470</RequestId>
  <LineItemTextLeft>Green Beans, canned</LineItemTextLeft>
  <LineItemTextRight>$0.59</LineItemTextRight>
  <LineItemRunningTextLeft>TOTAL</LineItemRunningTextLeft>
  <LineItemRunningTextRight>$1.19</LineItemRunningTextRight>
</SIP>
```

#### 5.3.8.5. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>LineItem</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<Responseld>	4-16N	Mandatory	See <a href="#">&lt;Responseld&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.8.6. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100470</RequestId>
  <Response>LineItem</Response>
  <ResponseId>100470</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
</SIP>

```

### 5.3.9. Notification Message

Notification messages are unsolicited messages sent by the SIP device to the POS at key points during a transaction.

Notification messages are used in the context of the StartCard command to communicate to the POS when the card has been acquired.

#### 5.3.9.1. Notification Enablement

The POS NOTIFICATION MESSAGES (**POSNOTIFY**) parameter determines if notification messages are enabled as follows:

POSNOTIFY	Meaning
0 (OFF)	HPA will not send notification messages to the POS
1 (ON)	HPA will send notification messages to the POS

#### 5.3.9.2. <Status> Element

The <Status> element in the notification message indicates the type of information being sent to the POS as follows:

Element Value	Definition
CARD PRESENTED	Card has been inserted, tapped, or swiped
CARD REMOVED EARLY	EMV card removed prematurely

APPLICATION SELECTION	Waiting for cardholder to select application for EMV contact card
APPLICATION SELECTED	Cardholder selected application
APPLICATION CONFIRMATION	Waiting for cardholder to confirm EMV application
APPLICATION CONFIRMED	Cardholder confirmed application
PROMPTING FOR PIN	Waiting for cardholder to enter PIN
PIN ENTERED	Cardholder has entered PIN
PIN BYPASSED	Cardholder chose to not enter PIN
AUTHORIZING	SIP device sending authorization request
PROMPTING FOR SIGNATURE	Waiting for cardholder to enter signature (Lane/5000 only)
SIGNATURE ENTERED	Cardholder has entered signature (Lane/5000 only)

**NOTE:** Currently only CARD PRESENTED is supported.

#### 5.3.9.3. Request Schema

There is no request for the notification message. It is an unsolicited message sent by the SIP device to the POS at key points during a transaction.

#### 5.3.9.4. Response Schema for CARD PRESENTED

At idle when a card is presented to HPA, a Card Presented notification message is sent to the POS utilizing these XML elements.

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<Response>	<b>Notification</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>

<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<Status>	<b>CARD PRESENTED</b>	Mandatory	See <Status>
<CardGroup>	1-6X	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
<CardType>	1-16X	Mandatory	See <a href="#">&lt;CardType&gt;</a>
<CardAcquisition>	1-7X	Mandatory	See <a href="#">&lt;CardAcquisition&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.9.5. Response Example for CARD PRESENTED

An example of such a message sent to the POS when a card is presented to HPA at idle is as follows.

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <Response>Notification</Response>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <Status>CARD PRESENTED</Status>
  <CardGroup>CREDIT</CardGroup>
  <CardType>MASTERCARD</CardType>
  <CardAcquisition>INSERT</CardAcquisition>
</SIP>

```

### 5.3.9.6. Notification Messages for Unsupported Status Element Values

Since the HPA only supports one Status element value, there are scenarios in which a Notification message will be sent without a Status element to handle cases for which a Status element is not supported.

For example if a StartCard card command is sent and an EMV card is removed too soon, then a Notification message will be sent without a Status element with a ResultText of CARD REMOVED TOO SOON.

Also, if a StartCard command is sent followed by a Reset or the Cancel key is pressed, SIP will send a Notification message without a Status element but with the ResultText set to TRANSACTION CANCELED

BY CLERK or TRANSACTION CANCELED BY CUSTOMER. This Notification message is sent even if POSNOTIFY is disabled.

### 5.3.10. Refund Command

This command will instruct HPA to perform a Refund transaction. HPA can refund full or partial of a previously approved financial transaction to release the hold on cardholder funds. The refund can be done with or without using the TransactionId of the original transaction. The following transactions can be refunded:

- Credit Sale
- Credit Auth
- Credit Voice Auth
- Debit Sale
- EBT FoodStamp Sale

The following rules apply when refunding by TransactionId of the original transaction:

- The total of all refunds cannot exceed the original sale amount. This is true for processing a single return as well as multiple returns against the same original transaction.
- Reversal, Void and CreditTransactionEdit(AdjustTip, CreditAdjustTip and TransactionAdjust) are not allowed against original transactions for which a full or partial refund has been performed.
- Refund is not allowed if the original transaction already voided.
- Refund can be voided.
- EBT FoodStamp refund is not allowed using TransactionId of the original EBT FoodStamp Sale.

#### 5.3.10.1. SAF Processing

Refunds will be processed as SAF per the Store-and-Forward (SAF) Mode (**STORMD**) parameter as indicated in the table below.

Value	Description
0 (OFF)	If the original transaction being refunded is in SAF pending state, the refund will be processed as SAF. Otherwise the refund will be attempted online, and will not be processed as SAF if host communications fail.
1 (ALWAYS)	All credit refunds will be processed as SAF.
3 (AUTO)	If the original transaction being refunded is in SAF pending state, the refund will be processed as SAF. Otherwise the refund will be attempted online, and credit refunds will be processed as SAF if host communications fail.

**NOTE:** Debit and EBT Refunds cannot be processed as SAF. Gift transactions cannot be refunded.



### 5.3.10.2. Processing Errors

The general processing errors that may occur for Refunds are:

- SIP TO HOST COMMUNICATION ERROR: Communication issue with host and the transaction cannot be SAFed.
- UNABLE TO ADJUST TIP AS ORIGINAL TRANSACTION HAS A REFUND AGAINST IT: The transaction is not allowed to edit.
- UNABLE TO VOID AS ORIGINAL TRANSACTION HAS A REFUND AGAINST IT: The transaction is not allowed to void.
- UNABLE TO REFUND AS ORIGINAL TRANSACTION IS INVALID: The transaction is invalid.
- UNABLE TO REFUND AS AMOUNT TO BE REFUNDED EXCEEDS THE ORIGINAL AMOUNT: The total of all refunds exceeds the original sale amount.

### 5.3.10.3. Refund Flow

Please refer to the [Subsequent Transactions](#) section for more information on the refund transaction flow.

### 5.3.10.4. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>Refund</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<TransactionId>	4-16N	Optional	See <a href="#">&lt;TransactionId&gt;</a>
<EBTAmount>	1-7N	Optional	See <a href="#">&lt;EBTAmount&gt;</a>
<TotalAmount>	1-7N	Mandatory	See <a href="#">&lt;TotalAmount&gt;</a>
<CardGroup>	All/Credit/Debit/EBT	Conditional If <TransactionId> used	See <a href="#">&lt;CardGroup&gt;</a>
<ConfirmAmount>	1N	Mandatory	See <a href="#">&lt;ConfirmAmount&gt;</a>
<InvoiceNbr>	1-25A	Optional	See <a href="#">&lt;InvoiceNbr&gt;</a>
<SignaturePrompt>	1N	Optional	See <a href="#">&lt;SignaturePrompt&gt;</a>

<code>&lt;/SIP&gt;</code>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
---------------------------	----	-----------	---------------------------------

### 5.3.10.5. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>Refund</Request>
  <RequestId>100486</RequestId>
  <TransactionId>1171913446</TransactionId>
  <EBTAmount>3504</EBTAmount>
  <TotalAmount>5504</TotalAmount>
  <CardGroup>All</CardGroup>
  <ConfirmAmount>0</ConfirmAmount>
  <SignaturePrompt>0</SignaturePrompt>
</SIP>

```

### 5.3.10.6. Response Schema

XML Element	Value	Usage	Description
<code>&lt;SIP&gt;</code>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<code>&lt;Version&gt;</code>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<code>&lt;ECRId&gt;</code>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<code>&lt;SIPId&gt;</code>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<code>&lt;DeviceId&gt;</code>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<code>&lt;RequestId&gt;</code>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<code>&lt;Response&gt;</code>	<b>Refund</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<code>&lt;ResponseId&gt;</code>	1-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<code>&lt;MultipleMessage&gt;</code>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<code>&lt;Result&gt;</code>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<code>&lt;ResultText&gt;</code>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<code>&lt;TransactionTime&gt;</code>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>
<code>&lt;GatewayRspCode&gt;</code>	1-4N	Conditional If returned by host	See <a href="#">&lt;GatewayRspCode&gt;</a>

<GatewayRspMsg>	1-34X	Conditional If returned by host	See <a href="#">&lt;GatewayRspMsg&gt;</a>
<ResponseCode>	2N	Conditional If host response received	See <a href="#">&lt;ResponseCode&gt;</a>
<ResponseText>	16X	Conditional If host response received	See <a href="#">&lt;ResponseText&gt;</a>
<ApprovalCode>	6N	Conditional If approved	See <a href="#">&lt;ApprovalCode&gt;</a>
<ReferenceNumber>	4-16N	Conditional If approved	See <a href="#">&lt;ReferenceNumber&gt;</a>
<CardholderName>	28X	Conditional If read from card	See <a href="#">&lt;CardholderName&gt;</a>
<CardType>	16X	Conditional If card acquired	See <a href="#">&lt;CardType&gt;</a>
<CardGroup>	1-6X	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
<CardAcquisition>	7X	Conditional If card acquired	See <a href="#">&lt;CardAcquisition&gt;</a>
<MaskedPAN>	16N or 19N	Conditional If card acquired	See <a href="#">&lt;MaskedPAN&gt;</a>
<SignatureLine>	1N	Conditional If approved	See <a href="#">&lt;SignatureLine&gt;</a>
<PinVerified>	1N	Conditional If approved	See <a href="#">&lt;PinVerified&gt;</a>
<AvailableBalance>	9N	Conditional If EBT refund	See <a href="#">&lt;AvailableBalance&gt;</a>
<AuthorizedAmount>	1-7N	Mandatory	See <a href="#">&lt;AuthorizedAmount&gt;</a>
<PartialApproval>	1N	Conditional if partially approved	See <a href="#">&lt;PartialApproval&gt;</a>

<BalanceDueAmount>	1-7N	Conditional if partially approved	See <a href="#">&lt;BalanceDueAmount&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.10.7. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100486</RequestId>
  <Response>Refund</Response>
  <ResponseId>1024543182</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>090817013452</TransactionTime>
  <GatewayRspCode>0</GatewayRspCode>
  <GatewayRspMsg>Success</GatewayRspMsg>
  <ResponseCode>00</ResponseCode>
  <ResponseText>APPROVAL</ResponseText>
  <ApprovalCode>72573A</ApprovalCode>
  <CardholderName>UATUSA/TESTCARD01</CardholderName>
  <CardType>VISA</CardType>
  <CardGroup>CREDIT</CardGroup>
  <CardAcquisition>SWIPE</CardAcquisition>
  <MaskedPAN>*****0119</MaskedPAN>
  <SignatureLine>0</SignatureLine>
  <PinVerified>0</PinVerified>
  <AuthorizedAmount>5504</AuthorizedAmount>
</SIP>

```

### 5.3.11. Reset Command

This command is used for two purposes: it is used to terminate a previously issued command such as a Sale transaction, and it is used to return the terminal to the idle state. The idle state can be “Lane Opened” state or a “Lane Closed” state.

It is important to understand that financial transaction result text such as APPROVED, DECLINED, or UNABLE TO PROCESS does not time out but is displayed until the POS sends a Reset command to clear the display and return the terminal to the idle state. The POS controls how long the transaction result text is displayed by the amount of time it waits after receiving the transaction response message before sending the Reset command.

During a financial transaction the POS may send a Reset command to cancel the transaction. If the Reset is successful (i.e. ResultText element is SUCCESS) then the terminal will cancel the transaction, display TRANSACTION CANCELED, send the Reset response followed by the transaction response message. The financial response message will have the ResultText element set to TRANSACTION CANCELED BY CLERK. The TRANSACTION CANCELED will continue to be displayed until the POS sends a Reset command to return the terminal to the idle state. Note that the flow is similar to normal financial transactions in that the POS sends a Reset command after receiving the transaction response message to clear the result text and return the terminal to the idle state.

To be clear, in the above scenario in which a Reset is used to cancel a Sale transaction there are two Resets sent by the POS. The first Reset cancels the transaction and is sent before the Sale response is received. The second Reset is sent after the Sale response is received and is used to clear the display and return the terminal to the idle state.

The Reset command must be sent after every financial transaction command (except for Start Card) after the response to the command is received. Failure to send a Reset command will result in the next command returning a SIP DEVICE BUSY error.

#### 5.3.11.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>Reset</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.3.11.2. Request Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>Reset</Request>
  <RequestId>100430</RequestId>
</SIP>
```

### 5.3.11.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>Reset</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	1-10N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.11.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100430</RequestId>
  <Response>Reset</Response>
  <ResponseId>100430</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
</SIP>

```

### 5.3.11.5. Card Acquisition Cancellation During StartCard

The StartCard command is used before a financial transaction to allow for card acquisition prior to the financial transaction being sent to the SIP device.

The SIP sends the StartCard response immediately to acknowledge that it has received the StartCard command and if POSNOTIFY is enabled will send a Notification message when the card data has been acquired.

If a Reset command is sent or the Cancel key is pressed on the terminal after StartCard, the terminal will display TRANSACTION CANCELED to inform the cardholder as to the reason why card acquisition is cancelled rather than simply returning to the idle state without explanation. A subsequent Sale or Refund transaction would also get canceled in this case.

Since the Reset command OR the Cancel key is triggering TRANSACTION CANCELED, the POS will need to send another Reset command to return the terminal to the idle state. Again, the POS controls how long the TRANSACTION CANCELED text is displayed to the cardholder by how long it waits before sending the next Reset command.

HPA sends a Notification message after the Cancel key is pressed OR it sends the response message to the Reset command. While it is possible to use this Notification message to trigger sending another Reset message to return to idle state, it is strongly recommended that the POS not rely on this Notification message.

**NOTE:** It is recommended that the POS send the second Reset based on the desired time to display the TRANSACTION CANCELED text and NOT rely on the Notification message.

## 5.3.12. Sale Command

This command initiates a Sale transaction.

### 5.3.12.1. Card Category Prompt

Refer to the [Card Type Determination](#) section.

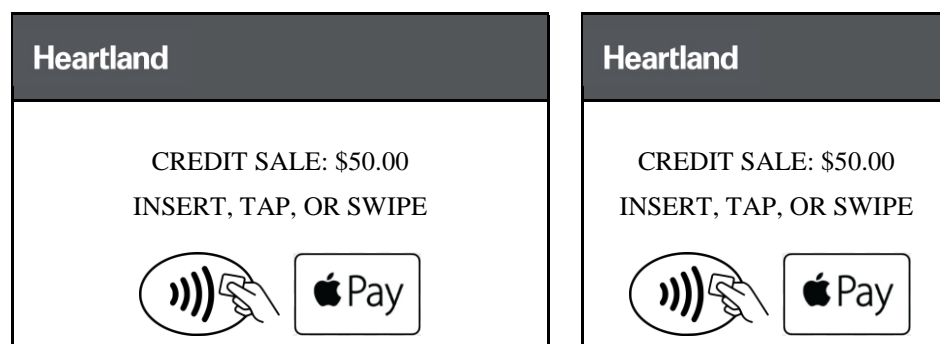
### 5.3.12.2. Card Acquisition Prompt

The card acquisition prompt will be displayed on the SIP device based on the CONTACTLESS READER (NFCRDR) parameter and one of the below conditions:

- The selected card category if card category prompt is enabled (**CRDCATPRMPT** = 1) or
- The values of <CardGroup> element enabled if card category prompt is disabled (**CRDCATPRMPT** = 0) or card category prompt is conditional (**CRDCATPRMPT**=2)

Card Category	NFCRDR Parameter	Card Acquisition Prompt
---------------	------------------	-------------------------

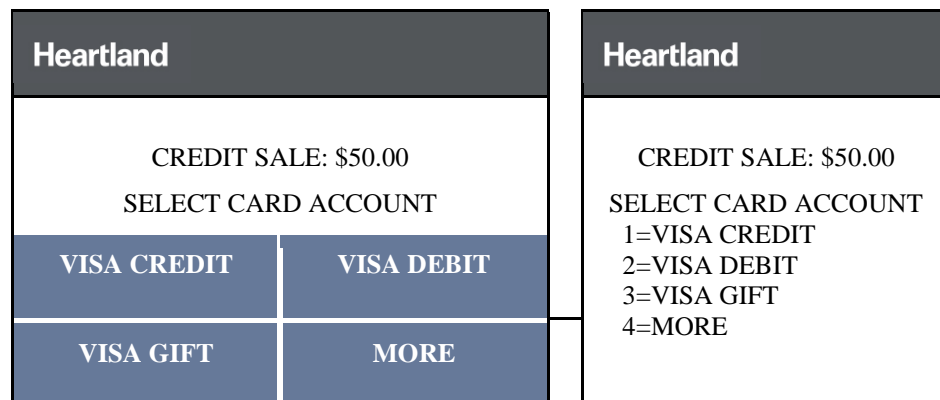
Credit, Debit	5 (INTERNAL)	INSERT, TAP, OR SWIPE
	0 (NONE)	INSERT OR SWIPE
Gift, or EBT	5 (INTERNAL)	SWIPE CARD
	0 (NONE)	SWIPE CARD



#### 5.3.12.3. Application Selection Prompt

If the card was inserted, and there are 2 or more applications on the chip that have different funding accounts, an application selection screen will appear to allow the cardholder to choose which account to use for payment.

A MORE button will appear if there are more than 3 underlying accounts to choose from.



**NOTE:** This prompt will be rare as most cards are only linked to 1 funding account.

#### 5.3.12.4. PIN Prompt

If the card was inserted, PIN is enabled, and the card is PIN preferring the cardholder will be prompted to enter their PIN.



**NOTE:** If the final amount is not yet known for the transaction, an amount will not be displayed, but an amount confirmation screen will be displayed prior to sending the sale to the host for authorization.

Heartland	Heartland
<p>CREDIT SALE: \$50.00</p> <p>ENTER PIN</p> <p>****</p>	<p>CREDIT SALE: \$50.00</p> <p>ENTER PIN</p> <p>****</p>

**NOTE:** If the cardholder presses the Cancel (X) key at this screen, HPA will proceed without PIN as a Credit transaction.

#### 5.3.12.5. Subsequent Processing

The commands that are permitted to follow StartCard, and that can be sent either during or after card acquisition are:

- Sale
- Refund
- Reset

If any other commands follow StartCard, HPA will respond with a “SIP DEVICE BUSY” result.

**NOTE:** If the transaction is canceled by the clerk, the POS must send a Reset command to ensure that the card data is not unintentionally used for an unassociated subsequent transaction.

#### 5.3.12.6. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>Sale</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-9N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>

<CardGroup>	1-21X	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
<ConfirmAmount>	1N	Mandatory	See <a href="#">&lt;ConfirmAmount&gt;</a>
<BaseAmount>	1-7N	Mandatory	See <a href="#">&lt;BaseAmount&gt;</a>
<TipAmount>	1-6N	Optional	See <a href="#">&lt;TipAmount&gt;</a>
<TaxAmount>	1-7N	Optional	See <a href="#">&lt;TaxAmount&gt;</a>
<EBTAmount>	1-7N	Optional	See <a href="#">&lt;EBTAmount&gt;</a>
<TotalAmount>	1-7N	Mandatory	See <a href="#">&lt;TotalAmount&gt;</a>
<TokenValue>	1-34X	Optional	See <a href="#">&lt;TokenValue&gt;</a>
<InvoiceNbr>	1-25X	Optional	See <a href="#">&lt;InvoiceNbr&gt;</a>
<TokenRequest>	1N	Optional	See <a href="#">&lt;TokenRequest&gt;</a>
<SignaturePrompt>	1N	Optional	See <a href="#">&lt;SignaturePrompt&gt;</a>
</SIP>		Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.12.7. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>Sale</Request>
  <RequestId>100410</RequestId>
  <CardGroup>Credit</CardGroup>
  <ConfirmAmount>1</ConfirmAmount>
  <BaseAmount>199</BaseAmount>
  <TipAmount>10</TipAmount>
  <TaxAmount>20</TaxAmount>
  <EBTAmount>229</EBTAmount>
  <TotalAmount>229</TotalAmount>
  <TokenRequest>1</TokenRequest>
  <SignaturePrompt>0</SignaturePrompt>
</SIP>

```

### 5.3.12.8. Response Schema

XML Element	Value	Usage	Description
-------------	-------	-------	-------------

<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>Sale</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<TransactionTime>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>
<GatewayRspCode>	1-4N	Conditional If returned by host	See <a href="#">&lt;GatewayRspCode&gt;</a>
<GatewayRspMsg>	1-34X	Conditional If returned by host	See <a href="#">&lt;GatewayRspMsg&gt;</a>
<ResponseCode>	2N	Conditional If returned by host	See <a href="#">&lt;ResponseCode&gt;</a>
<ResponseText>	16X	Conditional If returned by host	See <a href="#">&lt;ResponseText&gt;</a>
<ApprovalCode>	6N	Conditional If approved	See <a href="#">&lt;ApprovalCode&gt;</a>
<ReferenceNumber>	4-16N	Conditional If approved	See <a href="#">&lt;ReferenceNumber&gt;</a>
<CardholderName>	28X	Conditional If read from card	See <a href="#">&lt;CardholderName&gt;</a>
<CardType>	16X	Conditional If card acquired	See <a href="#">&lt;CardType&gt;</a>

<CardGroup>	1-6X	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
<CardAcquisition>	7X	Conditional If card acquired	See <a href="#">&lt;CardAcquisition&gt;</a>
<MaskedPAN>	15-19X	Conditional If card acquired	See <a href="#">&lt;MaskedPAN&gt;</a>
<EMV_AID>	10-32X	Conditional If EMV transaction	See <a href="#">&lt;EMV_AID&gt;</a>
<EMV_ApplicationName>	32X	Conditional If EMV transaction	See <a href="#">&lt;EMV_ApplicationName&gt;</a>
<EMV_TVR>	4X	Conditional If EMV transaction	See <a href="#">&lt;EMV_TVR&gt;</a>
<EMV_TSI>	4X	Conditional If EMV transaction	See <a href="#">&lt;EMV_TSI&gt;</a>
<EMV_CryptogramType>	2X	Conditional If EMV transaction	See <a href="#">&lt;EMV_CryptogramType&gt;</a>
<EMV_Cryptogram>	16X	Conditional If EMV transaction	See <a href="#">&lt;EMV_Cryptogram&gt;</a>
<SignatureLine>	1N	Conditional If approved	See <a href="#">&lt;SignatureLine&gt;</a>
<PinVerified>	1N	Conditional If approved	See <a href="#">&lt;PinVerified&gt;</a>
<TipAdjustAllowed>	1N	Mandatory	See <a href="#">&lt;TipAdjustAllowed&gt;</a>
<QPSQualified>	1N	Mandatory	See <a href="#">&lt;QPSQualified&gt;</a>
<AVSResultText>	1-32X	Conditional If returned by host	See <a href="#">&lt;AVSResultText&gt;</a>
<CVVResultText>	1-32X	Conditional If returned by host	See <a href="#">&lt;CVVResultText&gt;</a>
<AdditionalTipAmount>	9N	Conditional If additional tip was entered	See <a href="#">&lt;AdditionalTipAmount&gt;</a>

<TipAmount>	1-6N	Conditional If tip was sent from POS or entered by cardholder	See <a href="#">&lt;TipAmount&gt;</a>
<AvailableBalance>	9N	Conditional If EBT sale	See <a href="#">&lt;AvailableBalance&gt;</a>
<TaxAmount>	1-7N	Conditional If tax is enabled	See <a href="#">&lt;TaxAmount&gt;</a>
<AuthorizedAmount>	9N	Mandatory	See <a href="#">&lt;AuthorizedAmount&gt;</a>
<BalanceAmount>	9N	Conditional If Gift Sale	See <a href="#">&lt;BalanceAmount&gt;</a>
<TokenRspCode>	1-4N	Conditional If token requested	See <a href="#">&lt;TokenRspCode&gt;</a>
<TokenRspMsg>	1-34X	Conditional If token requested	See <a href="#">&lt;TokenRspMsg&gt;</a>
<TokenValue>	1-34X	Conditional If token requested	See <a href="#">&lt;TokenValue&gt;</a>
</SIP>		Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.12.9. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100410</RequestId>
  <Response>Sale</Response>
  <ResponseId>1024541600</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>090817041937</TransactionTime>
  <GatewayRspCode>0</GatewayRspCode>
  <GatewayRspMsg>Success</GatewayRspMsg>
  <ResponseCode>00</ResponseCode>
  <ResponseText>APPROVAL</ResponseText>
  <ApprovalCode>019883</ApprovalCode>

```

```

<ReferenceNumber>725113882553</ReferenceNumber>
<CardType>MASTERCARD</CardType>
<CardGroup>CREDIT</CardGroup>
<CardAcquisition>MSD TAP</CardAcquisition>
<MaskedPAN>*****4111</MaskedPAN>
<SignatureLine>0</SignatureLine>
<PinVerified>0</PinVerified>
<TipAdjustAllowed>1</TipAdjustAllowed>
<QPSQualified>0</QPSQualified>
<AdditionalTipAmount>0</AdditionalTipAmount>
<TipAmount>10</TipAmount>
<TaxAmount>20</TaxAmount>
<AuthorizedAmount>229</AuthorizedAmount>
<TokenRspCode>0</TokenRspCode>
<TokenRspMsg>Success</TokenRspMsg>
<TokenValue>JP21fN08Ed4QA9WkA14C0016</TokenValue>
</SIP>

```

**NOTE:** Token will not be generated for SAFed Sale request. So for SAFed Sale, response will contain a dummy Token response with:

```

<TokenRspCode>99</TokenRspCode>
<TokenRspMsg>Could Not Generate Token Offline</TokenRspMsg>

```

Token will not be generated for GIFT/EBT/Debit Sale transactions if Token is requested. Such transactions will receive dummy Token response as follows:

```

<TokenRspCode>98</TokenRspCode>
<TokenRspMsg>Cannot Request Token For Debit/EBT/Gift</TokenRspMsg>

```

In case of a successful Token response, the Token value will be saved by HeartPOS & later be used in successive Sale Request, with Card Acquisition mode as Token:

```

<CardAcquisition>Token</CardAcquisition>

```

#### 5.3.12.10. Gift Card Whitelist Sale

Gift card sales for which the card matches a BIN in the whitelist file are handled differently than normal sale transactions. HPA does not authorize the transaction but instead returns the track data back to the POS so that the POS may run the transaction. Gift card whitelist processing is enabled by setting the **WHITELIST** parameter TRUE.

##### 5.3.12.10.1. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>Sale</Request>
  <RequestId>100453</RequestId>
  <CardGroup>Gift</CardGroup>
  <ConfirmAmount>1</ConfirmAmount>
  <BaseAmount>400</BaseAmount>

```

```

    <TipAmount>0</TipAmount>
    <TaxAmount>0</TaxAmount>
    <TotalAmount>400</TotalAmount>
</SIP>

```

#### 5.3.12.10.2. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100453</RequestId>
  <Response>Sale</Response>
  <ResponseId>1024542597</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>090817044148</TransactionTime>
  <GatewayRspCode>0</GatewayRspCode>
  <GatewayRspMsg>Success</GatewayRspMsg>
  <ResponseCode>0</ResponseCode>
  <ResponseText>Success</ResponseText>
  <ApprovalCode>090804</ApprovalCode>
  <CardType>GIFT/REWARDS</CardType>
  <CardGroup>GIFT</CardGroup>
  <CardAcquisition>SWIPE</CardAcquisition>
  <MaskedPAN>*****0098</MaskedPAN>
  <SignatureLine>0</SignatureLine>
  <PinVerified>0</PinVerified>
  <TipAdjustAllowed>0</TipAdjustAllowed>
  <TipAmount>100</TipAmount>
  <TaxAmount>0</TaxAmount>
  <AuthorizedAmount>500</AuthorizedAmount>
</SIP>

```

#### 5.3.12.10.3. Whitelist Gift Card Sale Response

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <SIPIId>15293SC80802518</SIPIId>
  <DeviceId>6194404</DeviceId>
  <RequestId>[REQUEST ID]</RequestId>
  <Response>Sale</Response>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>022616153400</TransactionTime>
  <CardAcquisition>SWIPE</CardAcquisition>

```

```

<ClearPAN>6006496689000000001</ClearPAN>
<TrackNumber>2</TrackNumber>
<TrackData>6006496689000000001=25121019888877776</TrackData>
</SIP>

```

#### 5.3.12.10.4. Display Message Request

Since whitelist transactions are processed by the POS it is good practice for the POS to follow up the whitelist gift card sale with a Display message request so that the results of the POS processed transaction are displayed to the cardholder.

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <Request>Display</Request>
  <RequestId>[REQUEST ID]</RequestId>
  <DisplayString1>APPROVED</DisplayString1>
  <DisplayString2>TOTAL: </DisplayString2>
  <DisplayString3>$10.57</DisplayString3>
</SIP>

```

#### 5.3.12.10.5. Display Message Response

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <SIPIId>80812576</SIPIId>
  <DeviceId>6194404</DeviceId>
  <RequestId>[REQUEST ID]</RequestId>
  <Response>Display</Response>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>SUCCESS</ResultText>
</SIP>

```

### 5.3.13. StartCard Command

The POS may optionally send a StartCard command to HPA to display the card acquisition prompts on the SIP device prior to sending a financial transaction. This is intended to speed up transactions by allowing card acquisition to take place while sale items are still being rung up by the clerk.

**NOTE:** This feature cannot be used in conjunction with the line item feature.

**NOTE:** If the StartCard command is used, the determined card category will be used for the subsequent financial transaction, regardless of the <CardGroup> element specified in the transaction. If the determined card category is incompatible with the transaction (e.g. EBT CASH BENEFITS was selected and the subsequent transaction is a Refund), HPA will respond to the transaction with a “TRANSACTION NOT SUPPORTED” result.



### 5.3.13.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>StartCard</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<CardGroup>	1-21X	Optional	See <a href="#">&lt;CardGroup&gt;</a>
<TransactionType>	4-6X	Optional	See <TransactionType>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.13.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>StartCard</Request>
  <RequestId>100462</RequestId>
  <TransactionType>Sale</TransactionType>
  <CardGroup>Credit</CardGroup>
</SIP>

```

### 5.3.13.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>

<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>StartCard</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<Responseld>	4-16N	Mandatory	See <a href="#">&lt;Responseld&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.3.13.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100462</RequestId>
  <Response>StartCard</Response>
  <ResponseId>100462</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
</SIP>

```

### 5.3.14. TipAdjust Command

#### 5.3.14.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>TipAdjust</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<TransactionId>	4-16N	Mandatory	See <a href="#">&lt;TransactionId&gt;</a>

<TipAmount>	1-6N	Mandatory	See <a href="#">&lt;TipAmount&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.14.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>TipAdjust</Request>
  <RequestId>100459</RequestId>
  <TransactionId>1024697475</TransactionId>
  <TipAmount>111</TipAmount>
</SIP>

```

### 5.3.14.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Conditional If returned by host.	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>TipAdjust</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<TransactionTime>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>
<GatewayRspCode>	1-4N	Conditional If returned by host.	See <a href="#">&lt;GatewayRspCode&gt;</a>

<GatewayRspMsg>	1-34X	Conditional If returned by host.	See <a href="#">&lt;GatewayRspMsg&gt;</a>
<CardType>	16X	Mandatory	See <a href="#">&lt;CardType&gt;</a>
<CardGroup>	1-6X	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
<TipAmount>	1-6N	Mandatory	See <a href="#">&lt;TipAmount&gt;</a>
<TotalAmount>	1-7N	Mandatory	See <a href="#">&lt;TotalAmount&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.3.14.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPId>16322SC81188236</SIPId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100459</RequestId>
  <Response>TipAdjust</Response>
  <ResponseId>1024698368</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>091117082747</TransactionTime>
  <GatewayRspCode>0</GatewayRspCode>
  <GatewayRspMsg>Success</GatewayRspMsg>
  <CardType>MASTERCARD</CardType>
  <CardGroup>CREDIT</CardGroup>
  <TipAmount>111</TipAmount>
  <TotalAmount>260</TotalAmount>
</SIP>

```

#### 5.3.15. TransactionAdjust Command

The TransactionAdjust command is used to adjust the amount of a transaction. A common scenario is for it to be used to lower the base amount of a transaction, such as may arise if a manager wants to compensate a customer for an unsatisfactory experience.

The TransactionAdjust command adjusts the settlement amount of a transaction without going out to the issuer for authorization. While the TransactionAdjust command can be used to increase the amount of a transaction, if the transaction is raised more than the limits imposed by the card brands then the transaction may be subject to chargeback at settlement.

The TransactionAdjust command has three elements that define the transaction. The <TotalAmount> element should be the new adjusted total amount, not the amount of the adjustment. The Total Amount should include any tip amount. The command includes a <TipAmount> element, however this element is informational only. The third element is the <TransactionId> element. This element should be set to the value of the <ResponseId> element returned in the response of the transaction to be adjusted.

The TransactionAdjust command is applicable for the below transactions:

- Credit Sale
- Credit Auth
- Credit Voice Auth

The following rules apply TransactionAdjust:

- TransactionAdjust is not allowed if the original transaction already voided or refunded.
- Zero amount is not allowed for TransactionAdjust. To zero out a transaction use the Void command.

#### 5.3.15.1. SAF Processing

TransactionAdjust will be processed per the Store-and-Forward (SAF) Mode (STORMD) parameter as indicated in the table below and in the diagrams in the sections that follow.

Value	Description
0 (OFF)	All TransactionAdjust will be attempted online, and will not be processed as SAF if host communications fail. All TransactionAdjust will be processed as SAF if the associated transaction SAF approved.
1 (ALWAYS)	All TransactionAdjust will be processed as SAF.
3 (AUTO)	All TransactionAdjust will be attempted online, and all TransactionAdjust will be processed as SAF if host communications fail or associated transaction SAF approved.

#### 5.3.15.2. Processing Errors

The general processing errors that may occur for Refunds are:

- SIP TO HOST COMMUNICATION ERROR: Communication issue with host and the transaction cannot be SAFed.

- UNABLE TO ADJUST TRANSACTION AS ORIGINAL TRANSACTION HAS A REFUND AGAINST IT: The transaction is not allowed to adjust.
- UNABLE TO ADJUST TRANSACTION AS ORIGINAL TRANSACTION ALREADY VOIDED: The transaction is already voided.
- UNABLE TO ADJUST TRANSACTION AS ORIGINAL TRANSACTION IS INVALID: The transaction is invalid.

#### 5.3.15.3. TransactionAdjust Flow

Please refer to the [Subsequent Transactions](#) section for more information on the TransactionAdjust transaction flow.

#### 5.3.15.4. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>TransactionAdjust</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<TransactionId>	4-16N	Mandatory	See <a href="#">&lt;TransactionId&gt;</a>
<TotalAmount>	1-7N	Mandatory	See <a href="#">&lt;TotalAmount&gt;</a>
<TipAmount>	1-6N	Optional	See <a href="#">&lt;TipAmount&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.3.15.5. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <RequestId>1004160</RequestId>
  <Request>TransactionAdjust</Request>
  <TransactionId>1024844759</TransactionId>
  <TotalAmount>1150</TotalAmount>
  <TipAmount>250</TipAmount>
</SIP>

```

## 5.3.15.6. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-10N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>TransactionAdjust</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<Responseld>	1-10N	Mandatory	See <a href="#">&lt;Responseld&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<TransactionTime>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>
<GatewayRspCode>	1-4N	Conditional If returned by gateway.	See <a href="#">&lt;GatewayRspCode&gt;</a>
<GatewayRspMsg>	1-34X	Conditional If returned by gateway.	See <a href="#">&lt;GatewayRspMsg&gt;</a>
<ResponseCode>	2N	Conditional If host response received	See <a href="#">&lt;ResponseCode&gt;</a>
<ResponseText>	16X	Conditional If host response received.	See <a href="#">&lt;ResponseText&gt;</a>
<ReferenceNumber>	4-16N	Conditional If returned by the host	See <a href="#">&lt;ReferenceNumber&gt;</a>

<ApprovalCode>	6N	Conditional If returned by the host	See <a href="#">&lt;ApprovalCode&gt;</a>
<AvailableBalance>	9N	Conditional if balance returned by host	See <a href="#">&lt;AvailableBalance&gt;</a>
<AVSResultText>	1-32X	Conditional if balance returned by host	See <a href="#">&lt;AVSResultText&gt;</a>
<CVVResultText>	1-32X	Conditional If returned by host	See <a href="#">&lt;CVVResultText&gt;</a>
<AuthorizedAmount>	9N	Conditional If returned by host	See <a href="#">&lt;AuthorizedAmount&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.15.7. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>1004160</RequestId>
  <Response>TransactionAdjust</Response>
  <ResponseId>1024844766</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>091417110139</TransactionTime>
  <GatewayRspCode>0</GatewayRspCode>
  <GatewayRspMsg>Success</GatewayRspMsg>
  <ResponseCode>00</ResponseCode>
  <ResponseText>APPROVAL</ResponseText>
</SIP>

```

### 5.3.16. VoiceAuth Command

This command is used to initiate a Voice Authorized Sale transaction.

- The voice auth transaction is used when an authorization request returns a “Call for Auth” response code and the clerk calls the issuer to get the approval code.
- The application sends a CreditOfflineSale request to Portico to put the voice authorized transaction in the batch.



- The POS should send a six digit approval code in the VoiceAuth message to the SIP device.
- If a communication failure occurs the transaction is stored as a Store and Forward if it meets the SAF limits.
- AVS prompting, CVV2 prompting, Payment Selection, and QPS are not used for voice authorizations.

#### 5.3.16.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>VoiceAuth</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<ApprovalCode>	6X	Mandatory	See <a href="#">&lt;ApprovalCode&gt;</a>
<TotalAmount>	1-7N	Mandatory	See <a href="#">&lt;TotalAmount&gt;</a>
<SignaturePrompt>	1N	Optional	See <a href="#">&lt;SignaturePrompt&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.3.16.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>VoiceAuth</Request>
  <RequestId>100417</RequestId>
  <ApprovalCode>12345678</ApprovalCode>
  <TotalAmount>10000</TotalAmount>
  <SignaturePrompt>0</SignaturePrompt>
</SIP>

```

#### 5.3.16.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Conditional If returned by host.	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>VoiceAuth</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<TransactionTime>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>
<GatewayRspCode>	1-4N	Conditional If returned by host.	See <a href="#">&lt;GatewayRspCode&gt;</a>
<GatewayRspMsg>	1-34X	Conditional If returned by host.	See <a href="#">&lt;GatewayRspMsg&gt;</a>
<ResponseCode>	2N	Conditional if Host response received	See <a href="#">&lt;ResponseCode&gt;</a>
<ResponseText>	16X	Conditional if host response received.	See <a href="#">&lt;ResponseText&gt;</a>
<ApprovalCode>	6N	Conditional if Approved	See <a href="#">&lt;ApprovalCode&gt;</a>
<CardholderName>	28X	conditional If read from card	See <a href="#">&lt;CardholderName&gt;</a>
<CardType>	16X	Conditional If Card acquired	See <a href="#">&lt;CardType&gt;</a>
<CardGroup>	1-6X	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
<CardAcquisition>	7X	Conditional If Card acquired	See <a href="#">&lt;CardAcquisition&gt;</a>

<MaskedPAN>	16N or 19N	Conditional If Card acquired	See <a href="#">&lt;MaskedPAN&gt;</a>
<SignatureLine>	1N	Conditional if Approved	See <a href="#">&lt;SignatureLine&gt;</a>
<PinVerified>	1N	Conditional if Approved	See <a href="#">&lt;PinVerified&gt;</a>
<TipAdjustAllowed>	1N	Mandatory	See <a href="#">&lt;TipAdjustAllowed&gt;</a>
<AuthorizedAmount>	9N	Mandatory	See <a href="#">&lt;AuthorizedAmount&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 5.3.16.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100417</RequestId>
  <Response>VoiceAuth</Response>
  <ResponseId>1024692303</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>091117052541</TransactionTime>
  <GatewayRspCode>0</GatewayRspCode>
  <GatewayRspMsg>Success</GatewayRspMsg>
  <ResponseCode>00</ResponseCode>
  <ResponseText>APPROVAL</ResponseText>
  <ApprovalCode>123456</ApprovalCode>
  <CardholderName>UAT USA/Test Card 07</CardholderName>
  <CardType>MASTERCARD</CardType>
  <CardGroup>CREDIT</CardGroup>
  <CardAcquisition>INSERT</CardAcquisition>
  <MaskedPAN>*****4111</MaskedPAN>
  <SignatureLine>0</SignatureLine>
  <PinVerified>0</PinVerified>
  <TipAdjustAllowed>1</TipAdjustAllowed>
  <AuthorizedAmount>10000</AuthorizedAmount>
</SIP>

```

### 5.3.17. Void Command

This command is used to void a previously approved financial transaction that is still in the open batch to release the hold on cardholder funds. The following transactions can be voided:

- Credit Sale
- Credit Auth
- Credit Refund
- Credit Voice Auth
- Gift Sale
- Gift Add Value
- EBT FoodStamp Sale
- EBT FoodStamp Refund
- EBT CashBenefit Sale

**NOTE:** If the previously approved financial transaction is not allowed to be voided (e.g. a Debit transaction), or is in a batch that has already been closed, the Void will be rejected, and the only recourse to return funds to the cardholder account is to process a Refund transaction.

#### 5.3.17.1. SAF Processing

Store and Forward is available for Void transactions if the original transaction was a Credit Sale.

If a SAF approved transaction is voided, it will be marked as pending void in the SAF batch, and will no longer count against the SAF PENDING LIMIT (**STORLMT**) parameter used to determine how many pending SAF transactions are allowed.

Voids will be processed as SAF per the Store-and-Forward (SAF) Mode (**STORMD**) parameter as indicated in the table below and in the diagrams in the sections that follow.

Value	Description
0 (OFF)	If the original transaction being voided is in SAF pending state, the void will be processed as SAF. Otherwise the void will be attempted online, and will not be processed as SAF if host communications fail.
1 (ALWAYS)	All credit voids will be processed as SAF.
3 (AUTO)	If the original transaction being voided is in SAF pending state, the void will be processed as SAF. Otherwise the void will be attempted online, and credit voids will be processed as SAF if host communications fail.

#### 5.3.17.2. Processing Errors

The general processing errors that may occur for voids are:

- TRANSACTION NOT FOUND
  - The transaction being voided cannot be found on the Portico gateway.
- TRANSACTION ALREADY VOIDED
  - The transaction is already marked as voided or reversed on the Portico gateway.
- UNABLE TO VOID
  - The transaction being voided is a void transaction.
  - SAF Mode = 1 (ALWAYS) and the transaction being voided is an online approved credit sale and the card category of the original transaction was not provided.
- SIP TO HOST COMMUNICATION ERROR
  - Host communications fail and the void cannot be SAFed.

### 5.3.17.3. Void Flow

Please refer to the [Subsequent Transactions](#) section for more information on the void transaction flow.

### 5.3.17.4. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>Void</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<TransactionId>	4-16N	Mandatory	See <a href="#">&lt;TransactionId&gt;</a>
<TransactionIdType>	1-11X	Optional	See <a href="#">&lt;TransactionIdType&gt;</a>
<CardGroup>	1-21X	Optional	See <a href="#">&lt;CardGroup&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.17.5. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <Request>Void</Request>
  <RequestId>100411</RequestId>
  <TransactionId>1024676001</TransactionId>
  <TransactionIdType>RequestId</TransactionIdType>
  <CardGroup>Credit</CardGroup>
</SIP>

```

### 5.3.17.6. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Conditional If returned by host.	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>Void</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<ResponseId>	4-16N	Mandatory	See <a href="#">&lt;ResponseId&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<TransactionTime>	12N	Mandatory	See <a href="#">&lt;TransactionTime&gt;</a>
<GatewayRspCode>	1-4N	Conditional If returned by host.	See <a href="#">&lt;GatewayRspCode&gt;</a>
<GatewayRspMsg>	1-34X	Conditional If returned by host.	See <a href="#">&lt;GatewayRspMsg&gt;</a>
<ResponseCode>	2N	Conditional	See <a href="#">&lt;ResponseCode&gt;</a>

		If host response received	
<ResponseText>	16X	Conditional If host response received	See <a href="#">&lt;ResponseText&gt;</a>
<OrigTransactionId>	4-16N	Conditional If Void SAF	See <a href="#">&lt;OrigTransactionId&gt;</a>
<CardholderName>	28X	Conditional If read from the card	See <a href="#">&lt;CardholderName&gt;</a>
<CardGroup>	1-6X	Mandatory	See <a href="#">&lt;CardGroup&gt;</a>
<CardAcquisition>	7X	Conditional If card acquired	See <a href="#">&lt;CardAcquisition&gt;</a>
<BalanceAmount>	9N	Conditional If Gift void	See <a href="#">&lt;BalanceAmount&gt;</a>
<StoreAndForward>	1N	Conditional If SAF enabled and SAF approved.	See <a href="#">&lt;StoreAndForward&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 5.3.17.7. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>1004</ECRId>
  <SIPIId>16322SC81188236</SIPIId>
  <DeviceId>6225529</DeviceId>
  <RequestId>100411</RequestId>
  <Response>Void</Response>
  <ResponseId>1024688330</ResponseId>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>Success</ResultText>
  <TransactionTime>091117051354</TransactionTime>
  <GatewayRspCode>0</GatewayRspCode>
  <GatewayRspMsg>Success</GatewayRspMsg>
  <ResponseCode>00</ResponseCode>
  <OrigTransactionId>1153888240</OrigTransactionId>
  <CardGroup>CREDIT</CardGroup>
  <CardAcquisition>SWIPE</CardAcquisition>

```

```
<StoreAndForward>1</StoreAndForward>
</SIP>
```

## 5.4. XML Elements

### 5.4.1. <AdditionalTipAmount>

This element contains the tip amount entered by the cardholder in addition to the <TipAmount> from the POS.

Format	Length	Value
Numeric	1-6	Implied decimal point, no dollar sign, e.g. \$12.34 = 1234

### 5.4.2. <ApplicationId>

This element specifies the HUDS Application ID to download. If not specified, all applications associated with the Terminal ID will be downloaded.

Format	Length	Value
Alphanumeric	1-20	--

### 5.4.3. <ApprovalCode>

In the request, this element specifies the issuer approval code obtained over the phone for voice authorizations.

In the response, this element contains the issuer approval code returned by the host.

Format	Length	Value
Alphanumeric	6	--

### 5.4.4. <Attachment>

This element contains the status of sending attachments (i.e. signature data) to the host as part of EOD processing.

Format	Length	Value
Alphanumeric	1-32	e.g. "SUCCESS"



**5.4.5. <AttachmentData>**

This element contains the cardholder's signature data.

Format	Length	Value
Alphanumeric	var.	Base64 encoded BMP data

**5.4.6. <AuthorizedAmount>**

This element contains the amount authorized by the issuer as returned by the host.

Format	Length	Value
Numeric	1-7	Implied decimal point, no dollar sign, e.g. \$12.34 = 1234

**5.4.7. <AvailableBalance>**

This element contains the available balance of the card if <BalanceReturned> = 1.

Format	Length	Value
Numeric	1-7	Implied decimal point, no dollar sign, e.g. \$12.34 = 1234

**5.4.8. <AVS>**

This element contains the Address Verification Service (AVS) result code returned by the host.

Format	Length	Value
Alphanumeric	1	<b>Y:</b> Yes, address and zip are both correct. <b>N:</b> No, address and zip are both incorrect. <b>A:</b> Address only correct. <b>Z:</b> Zip only correct. <b>U:</b> Information unavailable. <b>S:</b> Address verification subscribed valid (not subscribed). <b>R:</b> System unavailable; retry. <b>L:</b> CM Name and Billing Zip match. <b>M:</b> CM Name, billing address and zip match. <b>O:</b> CM Name and billing address match. <b>K:</b> CM Name matches. <b>D:</b> CM Name incorrect, zip matches. <b>E:</b> CM Name incorrect, address and zip are both correct. <b>F:</b> CM Name incorrect, address correct. <b>W:</b> No, CM Name, address, and zip are all incorrect.

		0: Address verification was not requested.
--	--	--

#### 5.4.9. <AVSResultText>

This element contains a description of the AVS result.

Format	Length	Value
Alphanumeric	1-32	--

#### 5.4.10. <BalanceAmount>

This element contains the balance available on the card.

Format	Length	Value
Numeric	1-7	Implied decimal point, no dollar sign, e.g. \$12.34 = 1234

#### 5.4.11. <BalanceDueAmount>

This element contains the amount still due if the transaction was only partially approved.

Format	Length	Value
Numeric	1-7	Implied decimal point, no dollar sign, e.g. \$12.34 = 1234

#### 5.4.12. <BaseAmount>

This element specifies the base amount of the transaction before tips, taxes, and cashback are added.

Format	Length	Value
Numeric	1-7	Implied decimal point, no dollar sign, e.g. \$12.34 = 1234

#### 5.4.13. <BatchClose>

This element contains the status of sending the batch close request to the host as part of EOD processing.

Format	Length	Value
Alphanumeric	1-32	e.g. "SUCCESS"

#### 5.4.14. <ButtonText>

This element specifies the button text for the custom status form.

Format	Length	Value
Alphanumeric	1-8	--

#### 5.4.15. <CardAcquisition>

This element contains the method by which the card data was acquired.

Format	Length	Value
Alphanumeric	1-7	<b>Swipe:</b> Card was swiped through the magnetic stripe reader <b>Manual:</b> Card number was manually entered <b>Insert:</b> EMV card was inserted <b>Tap:</b> MSD or EMV contactless card was tapped <b>Token:</b> Token sent in place of card data

#### 5.4.16. <CardGroup>

This element is optional and is only applicable for Sale, Refund, Balance Inquiry, and Void Transactions. If not included then "All" will be used.

For a Void transaction the transaction is only eligible for Store and Forward if the CardGroup element is present and set to "Credit".

Multiple values may be included in the CardGroup element. For example, a Sale transaction may specify both Credit and Gift. The values should be separated by a space.

If the CardGroup specified is EBT, the SIP device will subsequently prompt the cardholder to select Food Stamp or Cash Benefits.

If multiple values are included, or the "All" value is specified, then HPA will prompt the cardholder to select the card type.

Format	Length	Value
Alphanumeric	1-21	<b>Credit:</b> Credit cards configured in HPA Card Table <b>Debit:</b> Debit cards configured in HPA Card Table <b>Gift:</b> Gift cards configured in HPA Card Table <b>EBT:</b> EBT cards configured in HPA Card Table <b>All:</b> Credit, Debit, Gift, and EBT

**5.4.17. <CardholderName>**

This element contains the name of the cardholder as obtained from the card.

Format	Length	Value
Alphanumeric	1-28	--

**5.4.18. <CardType>**

This element contains the card type.

Format	Length	Value
Alphanumeric	1-21	<b>Visa</b> <b>Mastercard</b> <b>American Express</b> <b>Discover</b> <b>EBT</b> <b>Gift</b> <Value from host>

**NOTE:** This tag will be excluded in response when token sale is SAFed and the same will get updated when it is sent online.

**5.4.19. <CashbackAmount>**

This element contains the cashback amount entered/selected by the cardholder.

Format	Length	Value
Numeric	1-7	Implied decimal point, no dollar sign, e.g. \$12.34 = 1234

**5.4.20. <ChoiceSelected>**

The text of the selected button will be returned.

Format	Length	Value
Alphanumeric	1-16	--

**5.4.21. <ClearPAN>**

This element contains the cleartext PAN as a result of whitelist processing.

**NOTE:** Whitelist processing only applies to gift cards which match BIN ranges defined in a signed whitelist file.

Format	Length	Value
Numeric	1-19	--

#### 5.4.22. <ConfirmAmount>

The element specifies if HPA should prompt the cardholder to confirm the amount. If not specified, a value of 0 (OFF) will be assumed.

Format	Length	Value
Boolean	1	<b>0</b> (OFF): Amount displayed but not explicitly confirmed <b>1</b> (ON): Cardholder will be prompted to confirm amount

#### 5.4.23. <CVV>

This element contains the Card Security Code (CVV2/CVC2/CID) result code returned by the host.

Format	Length	Value
Alphanumeric	1	<u>American Express</u> <b>M</b> : CID matches <b>N</b> : CID does not match <b>U</b> : CID was not checked  <u>Discover</u> <b>M</b> : CID matches <b>N</b> : CID does not match <b>P</b> : Not processed <b>S</b> : CID on card, but merchant says not CID on card <b>U</b> : Issuer not certified  <u>Mastercard</u> <b>M</b> : CVC2 matches <b>N</b> : No match <b>P</b> : Not processed <b>U</b> : Unregistered Issuer  <u>Visa</u> <b>M</b> : CVV2 matches <b>N</b> : CVV2 does not match <b>P</b> : Not processed

		<b>S:</b> Issuer says CVV2 on card but not provided in request <b>U:</b> Issuer not certified
--	--	--

#### 5.4.24. <CVVResultText>

This element contains a description of Card Security Code (CVV2/CVC2/CID) result.

Format	Length	Value
Alphanumeric	1-32	--

#### 5.4.25. <DataEntered>

This element returns the data entered by the cardholder.

Format	Length	Value
Alphanumeric	1-32	--

#### 5.4.26. <DateTime>

This element returns the date and time set successfully in SetClock.

Format	Length	Value
Numeric	14	Value must take this form YYYYMMDDHHMMSS

#### 5.4.27. <DeviceId>

This element contains the Device ID assigned to the terminal at boarding.

Format	Length	Value
Numeric	1-8	--

#### 5.4.28. <DownloadTime>

This element specifies when to initiate a download from HUDS.

Format	Length	Value
Alphanumeric	1-14	<b>NOW:</b> Initiate download immediately <b>EOD:</b> Initiate download after next EOD processing <b>YYYYMMDDHHMMSS:</b> Initiate download at specified date and time

### 5.4.29. <DownloadType>

This element specifies the type of download from HUDS.

Format	Length	Value
Alphanumeric	1-14	<b>FULL:</b> Download both software and parameters <b>PARTIAL:</b> Download only parameters <b>DIFFERENTIAL:</b> Download only those software and parameters associated to the Application IDs with software different from that on the terminal.

### 5.4.30. <EBTAmount>

This element specifies the amount of the transaction that qualifies for EBT purchase and refund. If the card type selected is EBT, this amount is sent to the host for approval. If it is less than <TotalAmount>, the transaction will be treated as a partial approval. EBT amount should never be greater than the <TotalAmount> in the transaction request.

Format	Length	Value
Numeric	1-7	Implied decimal point, no dollar sign, e.g. \$12.34 = 1234

### 5.4.31. <EBTType>

This element specifies the type of EBT transaction that should be run.

Format	Length	Value
Alphanumeric	1-12	<b>FoodStamp</b> <b>CashBenefits</b>

### 5.4.32. <ECRId>

This element specifies a POS defined unique identifier for the ECR, and it is echoed back by the SIP device to ensure that the response sent to the ECR is intended for that ECR workstation.

Format	Length	Value
Numeric	1-20	Must be non-zero

### 5.4.33. <EditBoxFormat>

This element specifies the format of the data entry field in the custom Edit Form used for obtaining input from the cardholder.

Format	Length	Value
Alphanumeric	1-32	<u>Formatting</u> <ul style="list-style-type: none"> <li>• X for alphanumeric</li> <li>• N for numeric</li> <li>• Any other character will be displayed as-is in the edit box and skipped for entry</li> <li>• No error checking is done on the format string</li> </ul> <u>Examples</u> <ul style="list-style-type: none"> <li>• NNN-NNN-NNNN: Social Security Number</li> <li>• (NNN) NNN-NNNN: Phone Number</li> <li>• NNNNN: 5-Digit Zip Code</li> <li>• NNNNN-NNNN: 9-Digit Zip+4 Code</li> <li>• NN/NN/NNNN: Date of Birth</li> </ul>

#### 5.4.34. <EMV\_AID>

For EMV transactions this element provides the AID of the EMV card so that the POS can print the AID on the receipt.

Format	Length	Value
Alphanumeric	1-32	Hexadecimal

#### 5.4.35. <EMV\_ApplicationName>

For EMV transaction this element provides the Preferred Name of the Application so that the POS can print the application name on the receipt. If the card does not provide the Preferred Name, or if the Issuer Code Table Index specifies an alphabet not supported by the system, then the Application Label provided by the card is used instead of the Preferred Name.

Format	Length	Value
Alphanumeric	1-16	ASCII

#### 5.4.36. <EMV\_Cryptogram>

For EMV transactions this element provides the cryptogram.

Format	Length	Value
Alphanumeric	1-16	Hexadecimal



**5.4.37. <EMV\_CryptogramType>**

For EMV transactions this element provides the cryptogram type (TC, AAR, AAC, or ARQC).

Format	Length	Value
Alphanumeric	1-16	ASCII

**5.4.38. <EMV\_TSI>**

For EMV transactions this element provides the Transaction Status Information tag (TSI).

Format	Length	Value
Alphanumeric	4	Hexadecimal

**5.4.39. <EMV\_TVR>**

For EMV transactions this element provides the Transaction Verification Results (TVR) register. This may be helpful in understanding why certain EMV transactions are declined.

Format	Length	Value
Alphanumeric	10	Hexadecimal

**5.4.40. <EMVOfflineDecline>**

Text description giving status of sending EMV Offline Decline messages to the host as part of EOD processing. Although HPA uses Quick Chip logic, it is possible for EMV cards to decline a transaction at the first cryptogram generation.

Format	Length	Value
Alphanumeric	1-32	ASCII

**5.4.41. <EMVPDL>**

Text description giving status of a possible EMV PDL performed as part of EOD processing.

Format	Length	Value
Alphanumeric	1-32	ASCII

**5.4.42. <EODEndTime>**

Date and time that the last EOD report request was completed.

Format	Length	Value
Numeric	12	Format is: MMDDYYHHMMSS

**5.4.43. <EODStartTime>**

Date and time that the last EOD report request was initiated.

Format	Length	Value
Numeric	12	Format is: MMDDYYHHMMSS

**5.4.44. <Field>**

This element is used to identify the beginning and end of a Key/Format pair.

Format	Length	Value
Alphanumeric	n/a	ASCII

**5.4.45. <FieldCount>**

This element is used in GetParameterReport, SetParameter and GetEMVParameterReport to identify how many parameters are sent in each SIP message.

Format	Length	Value
Numeric	1-2	Value may range from 1 to 30

**5.4.46. <FileName>**

This element is only used for SendFile, and is mandatory.

Format	Length	Value
Alphanumeric	1-14	Value may range from 1 to 14X

**5.4.47. <FileData>**

This element is only used for SendFile, and is mandatory.

Format	Length	Value
Alphanumeric	1-5120	Hexadecimal. Value may range from 1 to 5120X

**5.4.48. <FileSize>**

This element is only used for SendFile, and is mandatory.

Format	Length	Value
Numeric	1-7	File size in bytes. Maximum file size allowed is 1MB.

**5.4.49. <FormText>**

This element is used to define display prompt or body text for custom forms, and is mandatory

Display text may be restricted depending on the form type used. Please refer to the [Custom Forms](#) section for more details.

Format	Length	Value
Alphanumeric	1-2000	Value may range from 1 to 2,000X

**5.4.50. <GatewayRspCode>**

This element returns the response code provided by Portico. Please refer to the [Portico Gateway Response Codes](#) section for more details.

Format	Length	Value
Numeric	1-4	Response code from host

**5.4.51. <GatewayRspMsg>**

This element returns the response text to accompany the response code provided by Portico. Please refer to the [Portico Gateway Response Codes](#) section for more details.

Format	Length	Value
Alphanumeric	1-34	Response message from host

**5.4.52. <HeartBeat>**

Text description giving status of sending the HeartBeat message to the host as part of EOD processing.

Format	Length	Value
Alphanumeric	1-32	Indicates status of HeartBeat

**5.4.53. <HUDSPORT>**

This element is used for the Download command to provide the HUDS port. For Heartloader, the element is mandatory. For HPA, the element is optional.

Format	Length	Value
Numeric	1-4	Host port to use

**5.4.54. <HUDSURL>**

This element is used for Download command to provide the HUDS URL. For Heartloader, the element is mandatory. For HPA, the element is optional.

Format	Length	Value
Alphanumeric	1-128	Host URL to use

**5.4.55. <InvoiceNbr>**

This element is optional and applies to Sale, Refund, Voice Auth, and Credit Auth transactions.

Format	Length	Value
Numeric	1-25	Value may range from 1-25N

**5.4.56. <Key>**

This element is used to identify the data (parameter) which follows immediately in Value.

Format	Length	Value
Alphanumeric	1-32	Name of the parameter being set

**5.4.57. <LastResponse>**

This element is used in GetLastResponse to return the last stored response with an additional <StoredResponse>1</StoredResponse> flag to indicate that it is returning a stored response.

Format	Length	Value
Alphanumeric	var.	n/a

**5.4.58. <LeftButtonText>**

This element is used for custom Edit, Choice, and Signature forms, and is mandatory.

Format	Length	Value
Alphanumeric	1-8	Text to display on left button

**5.4.59. <LineItemRunningTextLeft>**

This element is used in LineItem to define left-justified display characters, which can overwrite right-justified characters on the same line if there is overlap.

Format	Length	Value
Alphanumeric	1-32	Left justified running text to display for all line items

**5.4.60. <LineItemRunningTextRight>**

This element is used in LineItem to define right-justified display characters, which can overwrite left-justified characters on the same line if there is overlap.

Format	Length	Value
Alphanumeric	1-32	Right justified running text to display for all line items

**5.4.61. <LineItemTextLeft>**

This element is used in LineItem to define left-justified display characters, such as purchase items.

Format	Length	Value
Alphanumeric	1-32	Left justified text to display for each line item

**5.4.62. <LineItemTextRight>**

This element is used in LineItem to define right-justified display characters, such as an item's sale price.

Format	Length	Value
Alphanumeric	1-32	Right justified text to display for each line item

**5.4.63. <MaskedPAN>**

This element is used to send the masked PAN to the POS so that it can be printed on the receipt. Every digit in the PAN is masked except for the last four digits which are sent in the clear. The length of this string is equal to the number of digits in the PAN.

Format	Length	Value
Alphanumeric	16-19	Masked out all but the last four digits of the account number, e.g. *****0119

**5.4.64. <MaxDataSize>**

This element defines the maximum number of characters of file data in hexadecimal ASCII format that can be sent in each subsequent request for SendFile Command.

Format	Length	Value
Numeric	1-7	Maximum number of characters of file data in hexadecimal ASCII format that can be sent in each subsequent request.

**5.4.65. <MultipleMessage>**

Some responses such as batch reports require multiple messages to send all the data to the POS. This element is only used in response messages and is used to indicate if the POS should expect another response message.

Format	Length	Value
Numeric	1	<b>0</b> : Last message <b>1</b> : More messages coming

**5.4.66. <OrigTransactionId>**

Original Transaction ID of transaction mentioned in Void Request.

Format	Length	Value
Numeric	4-16	--

**5.4.67. <PartialApproval>**

This element only applies to Sale , Credit Auth and EBT Refund transactions. The element is set to “1” when the transaction was only partially approved. In this case the <AuthorizedAmount> element contains the amount that was authorized and the remaining balance due is returned in the BalanceDueAmount element.

Format	Length	Value
Numeric	1	Conditional if partially approved

**5.4.68. <PinVerified>**

This element is used to inform the POS whether the receipt should print “PIN VERIFIED”. The element is also set to “1” on some mobile transaction (e.g. MasterCard) that performs the CVM on the mobile device.

**NOTE:** EMV CVM Lists may specify both signature and PIN, hence this element is not mutually exclusive with the <SignatureLine> element.

Format	Length	Value
Numeric	1	<b>0:</b> Do not print PIN VERIFIED <b>1:</b> Print PIN VERIFIED

**5.4.69. <QPSQualified>**

This element specifies whether or not the card is approved for the Quick Payment Service allowing quick low-dollar purchases. A QPS transaction bypasses the need for getting a signature on credit sale transactions.

Format	Length	Value
--------	--------	-------

Numeric	1	<b>0:</b> Not qualified <b>1:</b> Qualified
---------	---	--

#### 5.4.70. <Record>

This element identifies the beginning and end of a TableCategory. Every <Record> in a response will have a TableCategory followed by 10 or less <Field> elements or 10 or less <Field> elements with no TableCategory.

**NOTE:** The XML defined from Record up repeats for each TableCategory as a “heading”; each in its own separate <SIP> XML message. Thus only TableCategories with their individual elements are shown going forward.

Format	Length	Value
Alphanumeric	n/a	ASCII

#### 5.4.71. <ReferenceNumber>

This element contains a reference number returned by the issuer for financial transactions.

Format	Length	Value
Numeric	4-16	Reference number returned by the processor or issuer

#### 5.4.72. <Request>

This element specifies the command to be executed.

Format	Length	Value
Alphanumeric	1-32X	<u>Admin Commands</u> <b>ManagerMenu:</b> Enter manager menu on SIP device <b>GetAppInfoReport:</b> Get HPA application information report <b>GetParameterReport:</b> Get HPA parameter report <b>GetEMVParameterReport:</b> Get EMV parameter report <b>GetSAFReport:</b> Get Store and Forward report <b>GetLastEODReport:</b> Get Last End of Day Report <b>GetBatchReport:</b> Get batch report <b>SendSAF:</b> Send pending Store and Forward transactions <b>Reboot:</b> Reboot the SIP device <b>LaneOpen:</b> Go to lane open state <b>SetParameter:</b> Set the HPA parameters (key/value pairs)



		<p><b>Reset:</b> Reset the SIP device back to idle state</p> <p><b>EOD:</b> Initiate End of Day processing</p> <p><b>SendFile:</b> Send a file to HPA (Logo, Banner image files etc.)</p> <p><b>Download:</b> Used to explicitly download new version of application or update parameters</p> <p><b>SetClock:</b> Used to set the terminal clock</p> <p><u>Transaction Commands</u></p> <p><b>Sale:</b> Perform a Sale Transaction, available for Credit, Debit, EBT, and Gift cards</p> <p><b>CardVerify:</b> Perform a Card Verify, available for Credit cards</p> <p><b>Refund:</b> Perform a Refund Transaction, available for Credit, Debit, and EBT cards</p> <p><b>Void:</b> Available for sale transaction that is in current batch</p> <p><b>VoiceAuth:</b> Perform a Voice Authorized Sale Transaction</p> <p><b>BalanceInquiry:</b> Perform Balance Inquiry, available for Gift</p> <p><b>AddValue:</b> Add value to a gift card</p> <p><b>LaneClose:</b> Go to Lane Close State</p> <p><b>Reset:</b> Aborts the transaction (if possible) and returns to a Lane Open state</p> <p><b>CreditAuth:</b> Authorizes a Credit card transaction</p> <p><b>CreditAuthComplete:</b> Adds previous authorization to batch</p> <p><b>GetCardData:</b> Prompts for card swipe, sends track data to POS if not bank card</p> <p><b>TipAdjust:</b> Add or change tip on a previously approved transaction</p> <p><b>TransactionAdjust:</b> Used to adjust base amount of a transaction</p> <p><b>CreditTipAdjust (deprecated):</b> Add or change tip on a previously approved transaction</p> <p><b>StatusForm:</b> Used to display a form with a prompt and button text</p> <p><b>ChoiceForm:</b> Used to display a form with multiple choices</p> <p><b>SignatureForm:</b> Used to obtain a signature</p> <p><b>EditForm:</b> Used to display a form to prompt for text entry</p> <p><b>LineItem:</b> Used to display a line of text before a financial transaction</p> <p><b>StartCard:</b> Used to request card acquisition before financial transaction</p>
--	--	---

#### 5.4.73. <RequestId>

This element is mandatory and is used by the POS to uniquely identify transactions. This element is sent in the request and is then echoed back to the POS in the transaction response.

Format	Length	Value
Numeric	1-12	POS defined field used to uniquely identify the request Echoed back by the SIP device in the response

### 5.4.74. <Response>

Indicates that this message is a response message. This element is used in response messages and mirrors the value sent in the <Request> element of the command from the POS.

Format	Length	Value
Alphanumeric	1-32X	<u>Admin Commands</u> <b>ManagerMenu:</b> Enter manager menu on SIP device <b>GetAppInfoReport:</b> Get HPA application information report <b>GetParameterReport:</b> Get HPA parameter report <b>GetEMVParameterReport:</b> Get EMV parameter report <b>GetSAFReport:</b> Get Store and Forward report <b>GetLastEODReport:</b> Get Last End of Day Report <b>GetBatchReport:</b> Get batch report <b>SendSAF:</b> Send pending Store and Forward transactions <b>Reboot:</b> Reboot the SIP device <b>LaneOpen:</b> Go to lane open state <b>SetParameter:</b> Set the HPA parameters (key/value pairs) <b>Reset:</b> Reset the SIP device back to idle state <b>EOD:</b> Initiate End of Day processing <b>SendFile:</b> Send a file to HPA (Logo, Banner image files etc.) <b>Download:</b> Used to explicitly download new version of application or update parameters <b>SetClock:</b> Used to set the terminal clock <u>Transaction Commands</u> <b>Sale:</b> Perform a Sale Transaction, available for Credit, Debit, EBT, and Gift cards <b>CardVerify:</b> Perform a Card Verify, available for Credit cards <b>Refund:</b> Perform a Refund Transaction, available for Credit, Debit, and EBT cards <b>Void:</b> Available for sale transaction that is in current batch <b>VoiceAuth:</b> Perform a Voice Authorized Sale Transaction <b>BalanceInquiry:</b> Perform Balance Inquiry, available for Gift <b>AddValue:</b> Add value to a gift card <b>LaneClose:</b> Go to Lane Close State <b>Reset:</b> Aborts the transaction (if possible) and returns to a Lane Open state <b>CreditAuth:</b> Authorizes a Credit card transaction <b>CreditAuthComplete:</b> Adds previous authorization to batch <b>GetCardData:</b> Prompts for card swipe, sends track data to POS if not bank card <b>TipAdjust:</b> Add or change tip on a previously approved transaction <b>TransactionAdjust:</b> adjust the base amount of a transaction <b>CreditTipAdjust (deprecated):</b> Add or change tip on a previously approved transaction <b>StatusForm:</b> Used to display a form with a prompt and button text

		<b>ChoiceForm:</b> Used to display a form with multiple choices <b>SignatureForm:</b> Used to obtain a signature <b>EditForm:</b> Used to display a form to prompt for text entry <b>LineItem:</b> Used to display a line of text before a financial transaction <b>StartCard:</b> Used to request card acquisition before financial transaction <b>Notification:</b> Unsolicited notification of activity on the SIP device
--	--	---

#### 5.4.75. <ResponseCode>

The ResponseCode is used to indicate approval or denial. The format is two character alphanumeric characters. These two numeric digits returned by the Host are based on processing state.

See [Result and Response Codes](#) for details.

Format	Length	Value
Numeric	2	ResponseCode tells if transaction is successful or not

#### 5.4.76. <ResponseId>

The POS needs this element to void or adjust any transaction.

- For online approvals, the Gateway Transaction ID is returned.
- For Store and Forward approvals, the RequestID from the POS is returned.

Format	Length	Value
Numeric	4-16	Transaction identifier from host or terminal

#### 5.4.77. <ResponseText>

This element is a variable length text field returned to accompany the ResponseCode with a maximum length of 32 characters in ASCII format. The response text is from the issuer for issuer approved transactions but may contain text from the Portico Gateway if the transaction did not reach the issuer.

Format	Length	Value
Alphanumeric	1-32	Indicates status of transactions such as "APPROVAL", or "DECLINED"

### 5.4.78. <Result>

This element contains the result of HPA processing. When the value is other than 0, it specifies a two part result code encoded as four digits.

- The first two digits identify the module or functionality
- The last two digits identify the status or error

Format	Length	Value (Result Code: Result Text)
Numeric	1-4	<p><b>0</b>: Success</p> <p><u>GENERIC</u></p> <p><b>1001</b>: TIMED OUT</p> <p><b>1002</b>: TRANSACTION CANCELED BY CLERK</p> <p><b>1003</b>: TRANSACTION CANCELED BY CUSTOMER</p> <p><b>1004</b>: OPERATION NOT SUPPORTED</p> <p><u>HEARTBEAT</u></p> <p><b>1201</b>: UNABLE TO PARSE HEARTBEAT RESPONSE</p> <p><b>1202</b>: HEARTBEAT SYSTEM ERROR</p> <p><b>1203</b>: HEARTBEAT SYSTEM ERROR</p> <p><b>1204</b>: HEARTBEAT NOT REQUIRED</p> <p><b>1205</b>: HEARTBEAT REQUEST ERROR</p> <p><b>1206</b>: HEARTBEAT COMM ERROR</p> <p><b>1207</b>: HEARTBEAT PARSE E ERROR</p> <p><b>1208</b>: HEARTBEAT SERVER REPORTED ERROR</p> <p><b>1209</b>: HEARTBEAT PARSE I ERROR</p> <p><b>1210</b>: HEARTBEAT DISPLAY ERROR</p> <p><b>1211</b>: HEARTBEAT MODEM DOWNLOAD ERROR</p> <p><b>1212</b>: HEARTBEAT TCP DOWNLOAD ERROR</p> <p><u>DOWNLOAD</u></p> <p><b>1301</b>: CANNOT DOWNLOAD DUE TO BATCH OPEN</p> <p><b>1302</b>: EMV PDL DOWNLOAD ERROR</p> <p><u>REPORT</u></p> <p><b>1401</b>: CANNOT GENERATE BATCH REPORT FOR EMPTY BATCH</p> <p><b>1402</b>: CANNOT GENERATE EMV PARAMETER REPORT AS EMV IS DISABLED</p> <p><b>1404</b>: GENERIC BATCH REPORT ERROR</p> <p><b>1405</b>: LAST EOD REPORT NOT PRESENT</p> <p><b>1406</b>: LAST RESPONSE NOT PRESENT</p> <p><u>SIP DEVICE</u></p>

	<p> <b>1501:</b> CANNOT PROCESS IN LANE CLOSE STATE  <b>1502:</b> CANNOT PROCESS IN LANE OPEN STATE  <b>1503:</b> INVALID XML REQUEST  <b>1504:</b> TRANSACTION NOT SUPPORTED  <b>1505:</b> INVALID AMOUNT  <b>1506:</b> RESET REJECTED  <b>1507:</b> SIP DEVICE BUSY  <b>1508:</b> TOTAL AMOUNT OUT OF BOUNDS  <b>1509:</b> TOTAL AMOUNT DOES NOT ADD UP  <b>1510:</b> ECRID MISSING IN REQUEST  <b>1511:</b> REQUEST TYPE MISSING  <b>1512:</b> REQUESTID MISSING IN REQUEST  <b>1513:</b> INVALID FORM TEXT  <b>1514:</b> HPA CONFIGURATION ERROR  <b>1515:</b> INVALID INPUT FORMAT  <b>1516:</b> INVALID TRANSACTION ID  <b>1517:</b> BASE AMOUNT LESS THAN MINIMUM BASE AMOUNT  <b>1518:</b> BASE AMOUNT GREATER THAN MAXIMUM BASE AMOUNT  <b>1519:</b> TAX AMOUNT LESS THAN MINIMUM TAX AMOUNT  <b>1520:</b> TAX AMOUNT GREATER THAN MAXIMUM TAX AMOUNT  <b>1521:</b> TIP AMOUNT LESS THAN MINIMUM TIP AMOUNT  <b>1522:</b> TIP AMOUNT GREATER THAN MAXIMUM TIP AMOUNT  <b>1523:</b> TOTAL AMOUNT LESS THAN MINIMUM TOTAL AMOUNT  <b>1524:</b> TOTAL AMOUNT GREATER THAN MAXIMUM TOTAL AMOUNT  <b>1525:</b> EBT AMOUNT MISSING IN REQUEST  <b>1526:</b> EBT AMOUNT GREATER THAN MAXIMUM EBT AMOUNT  <b>1527:</b> TOTAL AMOUNT MUST INCLUDE TIP AMOUNT  <b>1528:</b> ADDITIONAL AMOUNT LESS THAN MINIMUM ADDITIONAL AMOUNT  <b>1529:</b> TIP AMOUNT EXCEEDS TOTAL AMOUNT  <b>1530:</b> CARD MUST BE REMOVED </p> <p> <u>DISPLAY</u>  <b>2101:</b> INTERNAL ERROR AT DISPLAY  <b>2102:</b> ERROR AT PIN ENTRY </p> <p> <u>CARD ACQUISITION</u>  <b>2201:</b> CARD BLOCKED  <b>2202:</b> CARD REMOVED TOO SOON  <b>2203:</b> CARD NOT ALLOWED  <b>2204:</b> INVALID CARD CATEGORY  <b>2205:</b> EMV IS DISABLED </p>
--	--

		<p><u>COMMUNICATION / HOST</u></p> <p><b>2401:</b> SIP TO POS COMMUNICATION ERROR</p> <p><b>2402:</b> SIP TO HOST COMMUNICATION ERROR</p> <p><b>2403:</b> ERROR BUILDING HOST XML REQUEST</p> <p><b>2404:</b> CANNOT RECOGNIZE HOST RESPONSE</p> <p><b>2405:</b> SIP TO HOST COMMUNICATION ERROR</p> <p><b>2406:</b> SIP TO HOST COMMUNICATION ERROR</p> <p><b>2407:</b> SIP TO HOST COMMUNICATION ERROR</p> <p><b>2411:</b> ERROR REPORTED BY PORTICO</p> <p><b>2412:</b> PORTICO RESPONSE EXCEEDS RESPONSE BUFFER SIZE</p> <p><b>2441:</b> SIP TO HOST COMMUNICATION TIME OUT</p> <p><b>2471:</b> SIP TO HOST COMMUNICATION TIME OUT</p> <p><u>BATCH</u></p> <p><b>2501:</b> BATCH IS EMPTY</p> <p><b>2502:</b> BATCH IS FULL</p> <p><b>2503:</b> SETTLEMENT FAIL</p> <p><b>2504:</b> UNABLE TO PROCESS REQUEST AS SETTLEMENT STARTED</p> <p><b>2505:</b> UNABLE TO REPORT BATCH, REPORT EXCEEDS LIMIT</p> <p><b>2507:</b> BATCH CLOSE IS DISABLED</p> <p><u>STORE AND FORWARD</u></p> <p><b>2701:</b> SAF COUNT EXCEEDED</p> <p><b>2702:</b> SAF AMOUNT EXCEEDED</p> <p><b>2703:</b> NO SAF TRANSACTIONS TO SEND</p> <p><b>2704:</b> MUST BATCH AUTH PENDING SAFS</p> <p><b>2705:</b> BATCH AUTH FAILED</p> <p><b>2706:</b> GATEWAY SYSTEM ERROR</p> <p><b>2707:</b> AUTH HAS BEEN VOIDED</p> <p><u>TRANSACTION/FILE</u></p> <p><b>2901:</b> ENCRYPTION ERROR</p> <p><b>2902:</b> TRANSACTION NOT ALLOWED IN SAF ALWAYS MODE</p> <p><b>2931:</b> VOID NOT FOUND</p> <p><b>2932:</b> ALREADY VOIDED</p> <p><b>2933:</b> UNABLE TO VOID</p> <p><b>2941:</b> INVALID CREDIT BALANCE INQUIRY</p> <p><b>2951:</b> APPROVAL CODE MUST BE SIX DIGITS</p> <p><b>2942:</b> BALANCE INQUIRY NOT SUPPORTED FOR CREDIT CARD GROUP</p> <p><b>2943:</b> BALANCE INQUIRY NOT SUPPORTED FOR DEBIT CARD GROUP</p> <p><b>2944:</b> AUTH ALREADY COMPLETED</p>
--	--	--

		<b>2961:</b> UNABLE TO ADJUST TIP <b>2962:</b> TIP CANNOT BE ADJUSTED FOR THIS TRANSACTION <b>2963:</b> UNABLE TO ADJUST TIP AS TRANSACTION ALREADY VOIDED <b>2952:</b> FILE CREATE FAILED <b>2953:</b> XML TAG ERROR <b>2954:</b> FILE SIZE TOO LARGE <b>2955:</b> INVALID FILE NAME <b>2956:</b> FILE NAME MISSING <b>2957:</b> PACKET SIZE TOO LARGE <b>2958:</b> TRANSACTION CANCELED BY CLERK <b>2964:</b> DUPLICATE TRANSACTION <b>2965:</b> TRANSACTION CANCELLED <b>2967:</b> UNABLE TO ADJUST TIP AS ORIGINAL TRANSACTION HAS A REFUND AGAINST IT <b>2968:</b> UNABLE TO VOID AS ORIGINAL TRANSACTION HAS A REFUND AGAINST IT <b>2969:</b> UNABLE TO REFUND AS ORIGINAL TRANSACTION ALREADY VOIDED <b>2970:</b> UNABLE TO REFUND AS ORIGINAL TRANSACTION IS INVALID <b>2971:</b> UNABLE TO REFUND AS AMOUNT TO BE REFUNDED EXCEEDS THE ORIGINAL AMOUNT <b>2972:</b> UNABLE TO ADJUST TRANSACTION AS ORIGINAL TRANSACTION HAS A REFUND AGAINST IT <b>2973:</b> UNABLE TO ADJUST TRANSACTION AS ORIGINAL TRANSACTION ALREADY VOIDED <b>2974:</b> UNABLE TO ADJUST TRANSACTION AS ORIGINAL TRANSACTION IS INVALID  <u>SYSTEM</u> <b>3101:</b> SYSTEM ERROR: BATCH CORRUPTED <b>3110:</b> ERROR PROCESSING SIGNATURE
--	--	--

#### 5.4.79. <ResultText>

This element contains the result text corresponding to the result code returned in the <Result> element. See [<Result>](#) for more details.

Format	Length	Value
Alphanumeric	1-32	HPA error text

**5.4.80. <Reversal>**

Text description giving status of sending reversals to the host as part of EOD processing.

Format	Length	Value
Alphanumeric	1-32	Indicates status of reversal transaction

**5.4.81. <RightButtonText>**

This element is used for custom Edit, Choice, and Signature forms, and is mandatory.

Format	Length	Value
Alphanumeric	1-8	Text to display on right button

**5.4.82. <SendSAF>**

Text description giving status of sending store and forward transactions to the host as part of EOD processing.

Format	Length	Value
Alphanumeric	1-32	Indicates status of SendSAF command

**5.4.83. <ServerLabel>**

This element is only applicable to SplitTip, to provide customer-prompting labels for all servers/stylists sharing a tip.

Format	Length	Value
Alphanumeric	1-64	Value may range from 1 to 64X

**5.4.84. <SignatureLine>**

This element is used to inform the POS whether a signature line should be printed on the receipt.

Format	Length	Value
Numeric	1	0: Do not print signature line



		<b>1:</b> Print signature line
--	--	--------------------------------

#### 5.4.85. <SignaturePrompt>

This element allows the POS to indicate to the SIP whether or not to prompt for a signature. Applies to Sale, Refund, Voice Auth, Credit Auth, and Credit Auth Complete transactions. The default behavior is assumed if the element is not supplied.

Format	Length	Value
Numeric	1	<b>0:</b> Do not prompt customer for a signature <b>1:</b> Prompt customer for a signature

#### 5.4.86. <SIP>

All messages will begin with this element to identify the message as a SIP message.

Format	Length	Value
Alphanumeric	n/a	Identifies the message as a SIP message

#### 5.4.87. <SIPIId>

Contains the Serial Number of the SIP device. The POS (ECR) can tie this to the workstation connected.

A typical use case is where the POS is coded to look at the SIPIId and if it's the first time connected, store it at the POS, saying a particular ECRId is associated with this SIPIId. Subsequent responses are checked to see if they are coming from the same SIPIId. If the SIPIId is different, the POS can be coded to alert the attendant that a different SIP device is detected during the LaneOpen command and prompt to either override and continue or abort the transaction and ensure the correct SIP device is connected.

It is advised to perform the End of Day processing before a SIP device is switched between POS workstations or lanes.

Format	Length	Value
Alphanumeric	1-20	Contains the Serial Number of the SIP device

#### 5.4.88. <Status>

If the POSNOTIFY parameter is enabled then the SIP device will send Notification messages to the POS during financial transactions with the Status element specifying the current status of the transaction.

See [Notification Message](#) for more details.

Format	Length	Value
Alphanumeric	1-32	Indicates the type of information being sent to the POS, e.g. CARD PRESENTED

#### 5.4.89. <StoreAndForward>

This is an element used in response messages to indicate that the transaction was approved offline in Store and Forward mode.

Format	Length	Value
Numeric	1	0: Transaction was not approved offline 1: Transaction was approved offline and is pending approval

#### 5.4.90. <TableCategory>

This element identifies to which category the parameters which follow it belong.

Format	Length	Value
Alphanumeric	1-32	e.g. CARD TYPE PARAMETERS

#### 5.4.91. <TaxAmount>

This element only applies to Sale transactions and is optional.

Format	Length	Value
Numeric	1-7	Implied decimal point, no dollar sign, e.g. \$12.34 = 1234

#### 5.4.92. <TerminalId>

This element is only used for Download to provide the terminal ID to download, and is mandatory.

Format	Length	Definition
Alphanumeric	1-20	Specifies the Terminal ID to download

**5.4.93. <Time>**

This element is only used for SetClock, and is mandatory.

Format	Length	Value
Numeric	14	Value must take this form YYYYMMDDHHMMSS

**5.4.94. <TipAdjustAllowed>**

This element is used to inform the POS whether tip adjustment is allowed for the transaction.

**NOTE:** Tip adjustment is currently only allowed for Credit sale, Credit Auth and Voice Auth transactions.

Format	Length	Value
Numeric	1	<b>0:</b> Tip adjustment is not allowed for transaction. POS should not print a tip line on receipt <b>1:</b> Tip adjustment is allowed for transaction. POS may print a tip line on receipt

**5.4.95. <TipAmount>**

This element only applies to Sale transactions and is optional.

Format	Length	Value
Numeric	1-6	Implied decimal point, no dollar sign, e.g. \$12.34 = 1234

**5.4.96. <TokenRequest>**

This element is used to indicate that the POS would like to receive a token from the host to be used in place of the specified card data.

Format	Length	Value
Numeric	1	<b>0:</b> Token will not be requested <b>1:</b> Token will be requested

**5.4.97. <TokenRspCode>**

This element returns the response code provided by the host for the token request.

Format	Length	Value
Numeric	1-4	If token requested

#### 5.4.98. <TokenRspMsg>

This element returns the response text provided by the host for the token request.

Format	Length	Value
Alphanumeric	1-34	If token requested

#### 5.4.99. <TokenValue>

In the request message, this element is used to pass the token value to HPA.

In the response message, this element is used to return the token value which is generated as part of a token request to the POS.

Format	Length	Value
Alphanumeric	1-34	If token requested

#### 5.4.100. <TotalAmount>

This element applies to all financial transactions and is mandatory, except for Verify, Void and Balance Inquiry

Format	Length	Value
Numeric	1-7	Implied decimal point, no dollar sign, e.g. \$12.34 = 1234

#### 5.4.101. <TrackData>

This element is used in whitelist processing to send clear text track data (track one or two) to the POS.

The Whitelist logic prefers track two and sends track two whenever available. If track two is not available but track one is then track one will be sent. Note that whitelist processing only applies to gift cards which match BIN ranges defined in a signed whitelist file and does not match a known bank card.

Format	Length	Value
Alphanumeric	128	Clear Text track data if Whitelist Gift card

#### 5.4.102. <TrackNumber>

This element is used in whitelist processing to send the track number to the POS.

The Whitelist logic prefers track 2 and sends track 2 whenever available. If track 2 is not available but track 1 is then track 1 will be sent. Note that whitelist processing only applies to gift cards which match BIN ranges defined in a signed whitelist file and does not match a known bank card.

Format	Length	Value
Numeric	1	1: Track 1 is returned 2: Track 2 is returned

#### 5.4.103. <TransactionCertificate>

Text description giving status of sending transaction certificates to the host as part of EOD processing. This field is deprecated as HPA no longer sends transaction certificates to the host.

Format	Length	Value
Alphanumeric	1-32	Indicates status of TransactionCertificate

#### 5.4.104. <TransactionId>

This element is used to identify the transactions to be voided for the Void transaction.

For Portico, if a transaction goes through and then the Gateway Transaction ID is returned in ResponseId, if not, then the Client Transaction ID is returned in ResponseId.

The Client Transaction ID sent to Portico is the value of the RequestId element received from the POS.

Format	Length	Value
Numeric	4-16	Used to identify the previously approved transaction, e.g. <ResponseId> from the original transaction

**5.4.105. <TransactionIdType>**

This element is used to specify the type of <TransactionId> being used in the Void command.

Format	Length	Value
Alphanumeric	9-10	<p><b>RequestId:</b> The specified &lt;TransactionId&gt; is the &lt;RequestId&gt; sent by the POS in the request message for the original transaction being voided. This would typically be used if the POS did not receive a response from HeartSIP for the original transaction.</p> <p><b>ResponseId:</b> The specified &lt;TransactionId&gt; is the &lt;ResponseId&gt; received by the POS in the response message for the original transaction being voided.</p> <p><b>NOTE:</b> If this element is not specified, HeartSIP will assume that the &lt;TransactionIdType&gt; is a ResponseId.</p>

**5.4.106. <TransactionTime>**

This element provides the timestamp of the transaction. Note that the SIP device clock is maintained in sync with the host by setting the SIP device clock based on time stamps in the host response.

Format	Length	Value
Numeric	12	Timestamp in MMDDYYHHMMSS format

**5.4.107. <Value>**

This element is used to assign a value to the immediately preceding Key.

Format	Length	Value
Alphanumeric	1-128	Value may range from 1 to 128X

**5.4.108. <Version>**

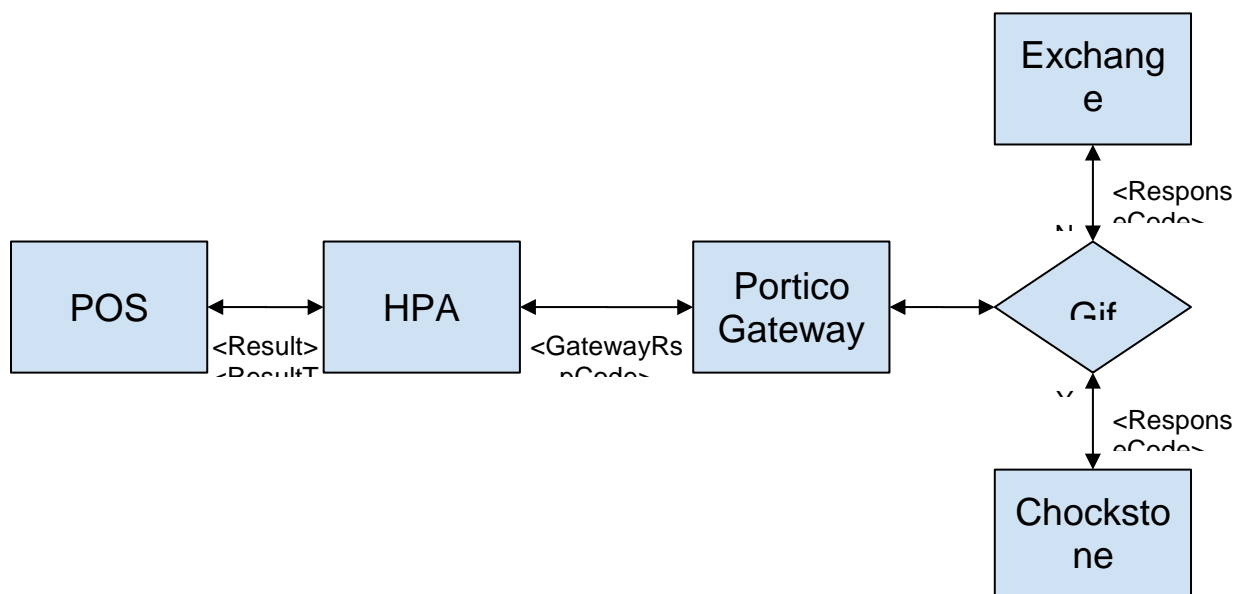
The current version of XML being used; for example, the 1.0 version.

Format	Length	Value
Numeric	1-2	Version in N.N format, e.g. <Version>2.0</Version>

## 5.5. Result and Response Codes

HPA returns several different XML response elements to indicate the overall success or failure of the transaction.

- **<Result>/<ResultText>**: Indicates the success or failure of HPA's processing of the request from the POS.
- **<GatewayRspCode>/<GatewayRspText>**: Indicates the success or failure of the Portico gateway's processing of the request from HPA.
- **<ResponseCode>/<ResponseText>**: Indicates the success or failure of the Exchange or Chockstone host's processing of the request from Portico.



### 5.5.1. HPA Error

If HPA fails to process the request from the POS and does not send the request to Portico, or successfully processes the request from the POS but does not get a response from Portico, the following XML elements will be included in the response to the POS:

XML Element	Value
<Result>	HPA error code (see <a href="#">HPA Result Codes</a> )
<ResultText>	HPA error text (see <a href="#">HPA Result Codes</a> )

### 5.5.2. Offline Decline

If HPA successfully processes the request from the POS but the transaction is declined offline by the EMV card, the following XML elements will be included in the response to the POS:

XML Element	Value
<Result>	0
<ResultText>	Success
<ResponseCode>	Offline response code (see <a href="#">Offline Response Codes</a> )
<ResponseText>	Offline response text (see <a href="#">Offline Response Codes</a> )

### 5.5.3. Gateway Error

If HPA successfully processes the request from the POS and sends the transaction to Portico, but Portico fails to process the request from HPA and does not send the transaction to Exchange/Chockstone, or successfully processes the request from HPA but does not get a response from Exchange/Chockstone, the following XML elements will be included in the response to the POS:

XML Element	Value
<Result>	0
<ResultText>	Success
<GatewayRspCode>	Portico error code (see <a href="#">Portico Gateway Response Codes</a> )
<GatewayRspMsg>	Portico error text (see <a href="#">Portico Gateway Response Codes</a> )

### 5.5.4. Store-and-Forward Response

If HPA successfully processes the request from the POS and the transaction is approved as Store-and-Forward, the following XML elements will be included in the response to the POS:

XML Element	Value
-------------	-------



<Result>	0
<ResultText>	Success
<ResponseCode>	00
<ResponseText>	APPROVAL
<StoreAndForward>	1

### 5.5.5. Host Response

If HPA successfully processes the request from the POS and sends the transaction to Portico, and Portico successfully process the request from HPA and sends the transaction to Exchange/Chockstone, and Exchange/Chockstone approves or declines the transaction, the following XML elements will be included in the response to the POS:

XML Element	Value
<Result>	0
<ResultText>	Success
<GatewayRspCode>	0
<GatewayRspMsg>	Success
<ResponseCode>	<b>For Credit/Debit/EBT:</b> See <a href="#">Exchange Host Response Codes</a> <b>For Heartland Gift:</b> See <a href="#">Chockstone Host Response Codes</a>
<ResponseText>	<b>For Credit/Debit/EBT:</b> See <a href="#">Exchange Host Response Codes</a> <b>For Heartland Gift:</b> See <a href="#">Chockstone Host Response Codes</a>

### 5.5.6. HPA Result Codes

<Result>	<ResultText>
0	Success

1001	TIMED OUT
1002	TRANSACTION CANCELED BY CLERK
1003	TRANSACTION CANCELED BY CUSTOMER
1004	OPERATION NOT SUPPORTED
1201	UNABLE TO PARSE HEARTBEAT RESPONSE
1202	HEARTBEAT SYSTEM ERROR
1203	HEARTBEAT SYSTEM ERROR
1204	HEARTBEAT NOT REQUIRED
1205	HEARTBEAT REQUEST ERROR
1206	HEARTBEAT COMM ERROR
1207	HEARTBEAT PARSE E ERROR
1208	HEARTBEAT SERVER REPORTED ERROR
1209	HEARTBEAT PARSE I ERROR
1210	HEARTBEAT DISPLAY ERROR
1211	HEARTBEAT MODEM DOWNLOAD ERROR
1212	HEARTBEAT TCP DOWNLOAD ERROR
1301	CANNOT DOWNLOAD DUE TO BATCH OPEN
1302	EMV PDL DOWNLOAD ERROR
1401	CANNOT GENERATE BATCH REPORT FOR EMPTY BATCH
1402	CANNOT GENERATE EMV PARAMETER REPORT AS EMV IS DISABLED
1404	GENERIC BATCH REPORT ERROR
1405	LAST EOD REPORT NOT PRESENT
1406	LAST RESPONSE NOT PRESENT
1501	CANNOT PROCESS IN LANE CLOSE STATE

1502	CANNOT PROCESS IN LANE OPEN STATE
1503	INVALID XML REQUEST
1504	TRANSACTION NOT SUPPORTED
1505	INVALID AMOUNT
1506	RESET REJECTED
1507	SIP DEVICE BUSY
1508	TOTAL AMOUNT OUT OF BOUNDS
1509	TOTAL AMOUNT DOES NOT ADD UP
1510	ECRID MISSING IN REQUEST
1511	REQUEST TYPE MISSING
1512	REQUESTID MISSING IN REQUEST
1513	INVALID FORM TEXT
1514	HPA CONFIGURATION ERROR
1515	INVALID INPUT FORMAT
1516	INVALID TRANSACTION ID
1517	BASE AMOUNT LESS THAN MINIMUM BASE AMOUNT
1518	BASE AMOUNT GREATER THAN MAXIMUM BASE AMOUNT
1519	TAX AMOUNT LESS THAN MINIMUM TAX AMOUNT
1520	TAX AMOUNT GREATER THAN MAXIMUM TAX AMOUNT
1521	TIP AMOUNT LESS THAN MINIMUM TIP AMOUNT
1522	TIP AMOUNT GREATER THAN MAXIMUM TIP AMOUNT
1523	TOTAL AMOUNT LESS THAN MINIMUM TOTAL AMOUNT
1524	TOTAL AMOUNT GREATER THAN MAXIMUM TOTAL AMOUNT
1525	EBT AMOUNT MISSING IN REQUEST

1526	EBT AMOUNT GREATER THAN MAXIMUM EBT AMOUNT
1527	TOTAL AMOUNT MUST INCLUDE TIP AMOUNT
1528	ADDITIONAL AMOUNT LESS THAN MINIMUM ADDITIONAL AMOUNT
1529	TIP AMOUNT EXCEEDS TOTAL AMOUNT
1530	CARD MUST BE REMOVED
2101	INTERNAL ERROR AT DISPLAY
2102	ERROR AT PIN ENTRY
2201	CARD BLOCKED
2202	CARD REMOVED TOO SOON
2203	CARD NOT ALLOWED
2204	INVALID CARD CATEGORY
2205	EMV IS DISABLED
2401	SIP TO POS COMMUNICATION ERROR
2402	SIP TO HOST COMMUNICATION ERROR
2411	ERROR REPORTED BY PORTICO
2403	ERROR BUILDING HOST XML REQUEST
2404	CANNOT RECOGNIZE HOST RESPONSE
2405	SIP TO HOST COMMUNICATION ERROR NOTE: Used when connect fails
2406	SIP TO HOST COMMUNICATION ERROR NOTE: Used when sending fails
2407	SIP TO HOST COMMUNICATION ERROR NOTE: Used when there is no response
2412	PORTICO RESPONSE EXCEEDS RESPONSE BUFFER SIZE
2441	SIP TO HOST COMMUNICATION TIME OUT

2471	SIP TO HOST COMMUNICATION TIME OUT
2501	BATCH IS EMPTY
2502	BATCH IS FULL
2503	SETTLEMENT FAIL
2504	UNABLE TO PROCESS REQUEST AS SETTLEMENT STARTED
2505	UNABLE TO REPORT BATCH, REPORT EXCEEDS LIMIT
2507	BATCH CLOSE IS DISABLED
2701	SAF COUNT EXCEEDED
2702	SAF AMOUNT EXCEEDED
2703	NO SAF TRANSACTIONS TO SEND
2704	MUST BATCH AUTH PENDING SAFS
2705	BATCH AUTH FAILED
2706	GATEWAY SYSTEM ERROR
2707	AUTH HAS BEEN VOIDED
2901	ENCRYPTION ERROR
2902	TRANSACTION NOT ALLOWED IN SAF ALWAYS MODE
2931	VOID NOT FOUND
2932	ALREADY VOIDED
2933	UNABLE TO VOID
2941	INVALID CREDIT BALANCE INQUIRY
2951	APPROVAL CODE MUST BE SIX DIGITS
2942	BALANCE INQUIRY NOT SUPPORTED FOR CREDIT CARD GROUP
2943	BALANCE INQUIRY NOT SUPPORTED FOR DEBIT CARD GROUP
2944	AUTH ALREADY COMPLETED

2961	UNABLE TO ADJUST TIP
2962	TIP CANNOT BE ADJUSTED FOR THIS TRANSACTION
2963	UNABLE TO ADJUST TIP AS TRANSACTION ALREADY VOIDED
2952	FILE CREATE FAILED
2953	XML TAG ERROR
2954	FILE SIZE TOO LARGE
2955	INVALID FILE NAME
2956	FILE NAME MISSING
2957	PACKET SIZE TOO LARGE
2958	TRANSACTION CANCELED BY CLERK
2964	DUPLICATE TRANSACTION
2965	TRANSACTION CANCELLED
2967	UNABLE TO ADJUST TIP AS ORIGINAL TRANSACTION HAS A REFUND AGAINST IT
2968	UNABLE TO VOID AS ORIGINAL TRANSACTION HAS A REFUND AGAINST IT
2969	UNABLE TO REFUND AS ORIGINAL TRANSACTION ALREADY VOIDED
2970	UNABLE TO REFUND AS ORIGINAL TRANSACTION IS INVALID
2971	UNABLE TO REFUND AS AMOUNT TO BE REFUNDED EXCEEDS THE ORIGINAL AMOUNT
2972	UNABLE TO ADJUST TRANSACTION AS ORIGINAL TRANSACTION HAS A REFUND AGAINST IT
2973	UNABLE TO ADJUST TRANSACTION AS ORIGINAL TRANSACTION ALREADY VOIDED
2974	UNABLE TO ADJUST TRANSACTION AS ORIGINAL TRANSACTION IS INVALID
3101	SYSTEM ERROR: BATCH CORRUPTED
3107	APPLICATION ERROR

3110	ERROR PROCESSING SIGNATURE
------	----------------------------

### 5.5.7. Offline Response Codes

<ResponseCode>	<ResponseText>	Notes
Z1	DECLINED BY CARD	EMV Offline Declined (before attempt to go online)

### 5.5.8. Portico Gateway Response Codes

<GatewayRspCode>	<GatewayRspMsg>	Notes
-21	UNAUTHORIZED	
-2	AUTHENTICATION ERROR	Verify and correct credentials.
-1	PORTICO ERROR	
0	SUCCESS	
1	GATEWAY SYSTEM ERROR	
2	DUPLICATE TRANSACTION	
3	INVALID TRANSACTION	
4	DUPLICATE TRANSACTION	
5	NO CURRENT BATCH	
6	INVALID RETURN AMOUNT	This can occur if a credit return request is against a specific original transaction and the return amount is greater than the original transactions settle amount, or the return amount is zero
7	INVALID REPORT PARMS	
8	BAD TRACK DATA	
9	TRANS NOT IN BATCH	
10	EMPTY REPORT	
11	NON CPC TRANS	

12	INVALID CPC DATA	
13	INVALID EDIT DATA	
14	INVALID CARD NUMBER	
15	BATCH CLOSE ACTIVE	
16	INVALID SHIP DATE	Transaction rejected because the ship date and month are invalid. Try again in a few seconds and resubmit
17	INVALID ENCRYPTION	
18	E3 MSR FAILURE	The message returned with this code is the parsed error message from the MSR data stream
19	INVALID REVERSAL AMOUNT	This can occur if a reversal request includes a new settlement amount that is not less than the current total authorization amount. The total authorization amount is the original authorization plus any incremental authorization minus any previous reversal amounts
20	DATABASE OP TIME-OUT	This may occur when Portico is trying to communicate to the database for large amounts of data. If this is due to a search, it can be corrected by adding more specific criteria
23	TOKENIZATION ERROR	An error was returned from the tokenization service when looking up a supplied token. This typically means that the provided token is bad, but it can also be returned when the data on the tokenization service has expired, been removed, or is no longer valid
24	TOKENS NOT SUPPORTED	This typically means that a token was supplied in the request but tokenization is not yet supported for the requested service type (see the section on tokenization for a list of supported services). This can also occur when tokenization is disabled for the entire system
25	TOKENS REJECTED	This error is returned if the merchant provides a



		token (TokenData.TokenValue) and requests a token (TokenRequest) in CardData. In this case, the transaction is rejected because a token cannot be presented and requested in the same request
26	BAD TOKEN ATTRIBUTES	This error is returned if there is an error setting the token attribute. When possible the tokenization service error/return code is returned in the message text
27	TOKEN NOT FOUND	This error is returned if the requested token was not found. This error can occur during TokenToPan (Lookup) or ManageTokens-Set (Update) requests
30	COMM FAILURE	This can occur when Portico does not receive a response from the back end systems and Portico is not sure if the transaction was successful or not
31	REVERSAL FAILURE	This occurs when Portico attempts a reversal for the POS, but the reversal fails. In this case, the POS is responsible for issuing the reversal
32	MISSING KTB	This can occur when a POS is attempting to send encrypted data, but the expected KTB value was corrupted or not received
33	MISSING KSN	This can occur when a POS is attempting to send encrypted data, but the expected KSN value was corrupted or not received
34	INVALID DATA RECVD	This error is returned from a CreditAuth or CreditSale if both GatewayTxnId and a CardData subfield are received
35	DEVICE SETTING ERROR	This error is returned from SendReceipt if the "AllowEmail" setting is not set to true for the device being used
36	INVALID ORIGINAL TRANS	This error is returned from a CreditAuth or CreditSale if the original transaction referenced

		by GatewayTxnId cannot be found. This is typically because the original does not meet the criteria for the sale or authorization by GatewayTxnID. This error can also be returned if the original transaction is found, but the card number has been written over with nulls after 30 days
37	MISSING ELEMENT	This error is returned if a required (or conditional) element is missing from the transaction
38	INVALID AUTH AMT	This error is returned from a CreditAuth or CreditSale by GatewayTxnId when the requested amount is over the threshold set for the transaction type, which is some percentage of the original amount (default = 100%)
39	INVALID EMV TLV DATA	Transaction rejected because EMV TLV data was invalid
40	INVALID REF TLV DATA	Transaction rejected because the referenced transaction has invalid EMV TLV data
41	FRAUD DETECTED	Transaction declined because possible fraud was detected
50	PROCESSOR SYS ERROR	
51	PROCESSOR CONFIG ERROR	

### 5.5.9. Exchange Host Response Codes

<ResponseCode>	<ResponseText>	Notes
00	APPROVAL	
02	CALL	No original no match. Often returned when the cardholder has exceeded daily credit limits/# of uses. Usually the Issuer wants to make sure the cardholder is still in possession of the card
03	TERM ID ERROR	Terminal ID error

04	HOLD-CALL	Retain card. Usually returned when the Issuer would like the merchant to take possession of the card due to potential fraud. Can also be returned if the transaction declines due to an AVS/CVV setting. The response text in this case is "DO NOT HONOR DUE TO AVS/CVV SETTINGS"
05	DECLINE	Do not honor. Normally occurs when cardholder has exceeded their allowable credit line
06	ERROR	Merchant closed no match
07	HOLD-CALL	
10	PARTIAL APPROVAL	
12	INVALID TRANS	
13	AMOUNT ERROR	Occurs when the POS submits an amount field equal to \$0.00. Re-enter transaction
14	CARD NO. ERROR	Card number error. Issuer cannot find the account. Re-enter transaction
15	NO SUCH ISSUER	Returned when the first six digits of the card number are not recognized by the Issuer. Reenter transaction
19	RE ENTER	Reenter transaction. Bad swipe
41	HOLD-CALL	Lost card
43	HOLD-CALL	Stolen card
44	HOLD-CALL	Pick up card
51	DECLINE	Insufficient funds
52	NO CHECK ACCOUNT	Occurs when the debit/check card being attempted is not linked to a Checking Account
53	NO SAVE ACCOUNT	Occurs when the debit/check card being used is not tied to a Savings Account
54	EXPIRED CARD	Card is expired. This response can also be returned in a Card Not Present environment if the cardholder tries to provide a valid expiration date, but the Issuer knows it is

		expired (indicates potential fraud)
55	WRONG PIN	Occurs in PIN-based Debit when the consumer enters the wrong 4-digit PIN
56	INVALID CARD	
57	SERV NOT ALLOWED	Service not allowed. Can be an incorrect MID or SIP device number, or attempt to process an unsupported card
58	SERV NOT ALLOWED	Service not allowed. Occurs when the POS attempts a transaction type that they are not set up for based on their MCC. (i.e., a merchant set up with a Direct Marketing MCC trying to perform a Debit transaction)
61	DECLINE	Occurs in PIN-based debit when the cardholder has exceeded their withdrawal limit when performing cashback
62	DECLINE	Occurs on swiped transactions when the Service Code encoded on the mag stripe does not equal the one stored at the Issuer (potential fraudulent card)
63	SEC VIOLATION	
65	DECLINE	Activity Limit. Occurs when the cardholder has exceeded the number of times the card can be used in a specific time period. (i.e., 10x in a 48 hr. span)
75	PIN EXCEEDED	Occurs when the number of attempts to enter the PIN has been exceeded
76	NO ACTION TAKEN	Occurs when the reversal data in the POS transaction does not match the Issuer data
77	NO ACTION TAKEN	Duplicate reversal or duplicate transaction
78	NO ACCOUNT	Account suspended, cancelled, or inactive
80	DATE ERROR	
82	CASHBACK NO APP	
85	CARD OK	

86	CANT VERIFY PIN	
91	NO REPLY	Time out
96	SYSTEM ERROR	
EB	CHECK DIGIT ERR	
EC	CID FORMAT ERROR	Format error
FR	FRAUD	Transaction declined because possible fraud was detected by Heartland
N7	CVV2 MISMATCH	Incorrect number of CVV2/CID digits sent

### 5.5.10. Chockstone Host Response Codes

<ResponseCode>	<ResponseText>	Notes
0	OK	Transaction successful
1	System error	Transaction unsuccessful because of an internal system error. Retry transaction. If the error persists, contact Heartland support.
2	System unavailable	Gift card system is temporarily unavailable. Retry transaction.
3	Invalid card	Transaction unsuccessful because the card is not a valid gift card.
4	Deactivated card	Do not honor. Normally occurs when cardholder has exceeded their allowable credit line
5	Insufficient funds	Merchant closed no match
6	Card already active	GiftCardActivate transaction unsuccessful because the gift card is already active.
7	Duplicate transaction	Transaction unsuccessful because a transaction with identical parameters was completed less than 3 minutes ago.
8	Inactive card	Transaction unsuccessful because the gift card is not active.

9	Invalid amount	Transaction unsuccessful because an invalid amount was specified.
10	Cannot void	
11	Unknown error	
12	Do not honor	
13	Partial approval	

## 5.6. SIP Response to POS Communication Failure

In the event that the POS sends a financial transaction to the SIP device, but the POS does not receive a response from the SIP device, the POS may re-send the message to the SIP device.

HPA will store the last response it attempted to send to the POS for the following financial transactions:

- Sale
- CardVerify
- Refund
- Void
- VoiceAuth
- BalanceInquiry
- AddValue
- GetCardData
- CreditAuth
- TipAdjust

**NOTE:** The response will be stored until another financial transaction command or the EOD command is sent to the SIP device.

If HPA has a response stored, and the POS sends a transaction to the SIP device where the <ECRId>, <Request> and <RequestId> element values match those in the stored response, HPA will simply return the stored response to the POS.

**NOTE:** In this case, HPA will include a <StoredResponse>1</StoredResponse> flag in the response to indicate that it is returning a stored response.

If HPA has a response stored, but the POS sends a transaction to the SIP device where the <ECRId>, <Request>, and <RequestId> element values do not match those in the stored response, or if HPA does not have a response stored at all, HPA will treat it as a new transaction and submit it to Portico for authorization.

### 5.6.1. Request Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <Request>Sale</Request>
  <RequestId>13986</RequestId>
  <CardGroup>Credit</CardGroup>
  <ConfirmAmount>0</ConfirmAmount>
  <BaseAmount>587</BaseAmount>
  <TipAmount>0</TipAmount>
  <TaxAmount>48</TaxAmount>
  <EBTAmount>635</EBTAmount>
  <TotalAmount>635</TotalAmount>
</SIP>
```

#### SIP Response To POS Communication Failure—POS Resends Request

```
<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <Request>Sale</Request>
  <RequestId>13986</RequestId>
  <CardGroup>Credit</CardGroup>
  <ConfirmAmount>0</ConfirmAmount>
  <BaseAmount>587</BaseAmount>
  <TipAmount>0</TipAmount>
  <TaxAmount>48</TaxAmount>
  <EBTAmount>635</EBTAmount>
  <TotalAmount>635</TotalAmount>
</SIP>
```

### 5.6.2. Response Example

```
<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <SIPId>15293SC80802518</SIPId>
  <DeviceId>6194404</DeviceId>
  <GatewayRspCode>0</GatewayRspCode>
  <GatewayRspMsg>Success</GatewayRspMsg>
  <Response>Sale</Response>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>SUCCESS</ResultText>
  <CardholderName>JCB TEST CARD</CardholderName>
  <CardAcquisition>SWIPE</CardAcquisition>
  <ResponseCode>00</ResponseCode>
  <ApprovalCode>001825</ApprovalCode>
```

```
<ResponseText>APPROVAL</ResponseText>
<RequestId>
</RequestId>
<ResponseId>605719319649</ResponseId>
<TransactionTime>022616152735</TransactionTime>
<MaskedPAN>*****0014</MaskedPAN>
<CardType>MASTERCARD</CardType>
<TipAdjustAllowed>1</TipAdjustAllowed>
<SignatureLine>1</SignatureLine>
<ReferenceNumber>[Number]</ReferenceNumber>
<PinVerified>0</PinVerified>
<AVSResultText>AVS Not Requested.</AVSResultText>
<AuthorizedAmount>635</AuthorizedAmount>
<QPSQualified>1</QPSQualified>
<StoredResponse>1</StoredResponse>
</SIP>
```



## 6. Heartland Payment Application Features

### 6.1. Quick Chip

Quick Chip speeds up EMV transaction processing to make the cardholder experience more similar to swiping a card, where they would insert their card and remove it after only a few seconds. This is accomplished in two key ways:

- It allows the EMV transaction flow, i.e. the interaction between the card and the terminal, to begin before the final amount of the transaction is known. This means that the card can be acquired, and by all methods including INSERT and TAP, while the sale items are still being rung up by the clerk.

**NOTE:** The StartCard command must be used to take advantage of the above facet of Quick Chip.

- It allows the EMV transaction flow to end prior to host messaging. This means that the card can be removed sooner, without having to wait for host communications and the post-authorization interaction with the card to complete.

**NOTE:** Quick Chip will be used for all U.S. deployments.

#### 6.1.1. Predetermined Amount

The QUICK CHIP AMOUNT (**QCHIPAMT**) parameter is used to specify the predetermined amount (in cents) that will be used for Quick Chip processing.

- If the StartCard command is used, HPA will provide this predetermined amount to the EMV kernel to initiate the EMV transaction flow.
- If the StartCard command is not used, then HPA will provide the amount specified in the financial transaction to the EMV kernel.
- If the StartCard command is used, QPS is enabled, and the predetermined amount is less than or equal to the QPS limit, then the CVM Results will indicate No CVM Required, and PIN will not be prompted. If the final transaction amount ends up being greater than the QPS limit, HPA will still perform the Signature CVM.

**NOTE:** If the card is PIN preferring, PIN is not prompted, and the final transaction amount is greater than the QPS limit, the merchant may be liable for lost/stolen fraud chargebacks.

- If the StartCard command is used, QPS is enabled, and the predetermined amount is greater than the QPS limit, then the CVM Results will indicate PIN or Signature based on the card's preference.
  - If the card prefers PIN, HPA will prompt for PIN.
 

**NOTE:** If PIN is prompted, the amount will not be shown at the PIN prompt, since the final transaction amount is not yet known at this point.
  - If the card prefers Signature, HPA will only perform the Signature CVM if the final transaction amount ends up being greater than the QPS limit.
  - If the StartCard command is used, and QPS is disabled, then the PIN or Signature CVM will be performed based on the card's preference, regardless of the predetermined amount.

The following table contains several examples that illustrate the application of the rules presented above in terms of the relationship between the predetermined amount (QCHIPAMT), the QPS limit, and the final transaction amount, and how those variables determine the expected CVM.

QCHIPAMT	QPS Limit	Transaction Amount	Expected CVM
\$1	\$50	\$40	No CVM Required
\$1	\$50	\$60	No PIN, only Signature
\$1	\$0 (disabled)	Any	PIN or Signature (per card preference)
\$51	\$50	\$40	No Signature, only PIN (if card is PIN-preferring)
\$51	\$50	\$60	PIN or Signature (per card preference)
\$51	\$0 (disabled)	Any	PIN or Signature (per card preference)

### 6.1.2. Internal Processing

The following does not impact the POS interface, but is important implementation information pertaining to HPA's internal processing of Quick Chip.

Quick Chip is online-only, meaning that the terminal must attempt to go online for authorization for all transactions. This has the following impacts:

- The terminal floor limits must be set to \$0 for all AIDs. This ensures that the terminal will request an ARQC cryptogram at the 1st GENERATE AC command so that it can go online for authorization for all transactions.

**NOTE:** If a non-\$0 floor limit is received in the EMV PDL, it must be overridden and set to \$0.

- If the card returns an AAC cryptogram at 1st GEN AC, the transaction has been offline declined by the card and must be terminated.
- If the card returns an ARQC cryptogram at 1st GEN AC, the terminal should store the ARQC and other associated chip data, and immediately request an AAC cryptogram at 2nd GEN AC by setting the Authorization Response Code to 'Z3' (unable to go online, offline declined). The terminal should then prompt the cardholder to remove their card, and send the ARQC to the host for online authorization.
- If the terminal cannot go online for authorization due to communication or host issue, it may still invoke SAF processing, but the card is no longer inserted therefore it cannot be asked for offline approval.

**NOTE:** Post-authorization processing such as Issuer Authentication and Issuer Script Processing is not performed with Quick Chip, as the card is no longer inserted after host communications.

## 6.2. Card Type Determination

### 6.2.1. <CardGroup> Element

A financial command may optionally contain the <CardGroup> element to specify the card categories that may be acquired. If the <CardGroup> element is not specified, then it is assumed that all card categories may be acquired.

Element Value(s)	Meaning
Credit	Credit cards configured in HPA Card Table
Debit	Debit cards configured in HPA Card Table
Gift	Gift cards configured in HPA Card Table
EBT	EBT cards configured in HPA Card Table

All	All Credit, Debit, Gift, and EBT cards configured in HPA Card Table
-----	---

Multiple values may be included in the <CardGroup> element, and must be separated by a space. For example, to accept either a Credit or Gift card for a transaction, <CardGroup>Credit Gift</CardGroup> would be used. If there are no cards configured in the HPA Card Table for the specified category it will be ignored.

If the POS specifies an explicit card category in the <CardGroup> element (e.g. <CardGroup>Credit</CardGroup>, <CardGroup>Debit</CardGroup>, etc.), HPA will run the transaction as such.

If the POS does not specify an explicit card category (e.g. no <CardGroup> element, <CardGroup>All</CardGroup>, <CardGroup>Credit Debit</CardGroup>, etc.), HPA will determine the card category based on the value of the CARD CATEGORY PROMPT (**CRDCATPRMPT**) parameter as detailed in this section.

### 6.2.2. CRDCATPRMPT = 0 (Disabled)

The card category prompt is not displayed, and after card acquisition the card category is assumed to be Credit or Gift as follows:

- If card inserted or tapped (EMV), run as Credit
- If card tapped (MSD), swiped, or manually entered:
  - If card in Credit BIN range, run as Credit
  - If Whitelist enabled, and card in Whitelist BIN range, run as Whitelist Gift
  - If Gift enabled, and card in Gift BIN range, run as Heartland Gift
  - If card not in any of the above BIN ranges:
    - If Gift enabled, run as Heartland Gift
    - If Gift disabled, prompt “CARD NOT SUPPORTED”

This option is intended for merchants who are limiting card acceptance to Credit and Gift due to the unavailability of a customer facing PIN pad such as at a drive-thru, therefore it is not recommended for Debit or EBT cards.

- If the POS sends an explicit Debit or EBT request (e.g. <CardGroup>Debit</CardGroup>), HPA will still run it as such, it just will not assume Debit or EBT.
- If the POS specifies a mix of Credit/Gift + Debit/EBT (e.g. <CardGroup>Credit Debit</CardGroup>), HPA will ignore the Debit/EBT part.
- If the POS specifies an incompatible mix of Debit/EBT (e.g. <CardGroup>Debit EBT</CardGroup>), HPA will immediately respond with “INVALID CARD CATEGORY”.

### 6.2.3. CRDCATPRMPT = 1 (Enabled)

The card category prompt is displayed prior to card acquisition. The card categories available for selection will vary based on the <CardGroup> element and which card categories are enabled in the application.

Heartland		Heartland
SELECT CARD TYPE		SELECT CARD TYPE
CREDIT	DEBIT	1=CREDIT
EBT	GIFT	2=DEBIT
		3=EBT
		4=GIFT

Heartland		Heartland
SELECT EBT TYPE		SELECT CARD TYPE
FOOD STAMP	CASH BENEFITS	1=FOOD STAMP
		2=CASH BENEFITS

### 6.2.4. CRDCATPRMPT = 2 (Conditional)

The card category prompt is conditionally displayed if the card category cannot be definitively determined after card acquisition based on the AIDs and/or BIN Ranges.

- If card inserted or tapped (EMV), run as Credit
- If card tapped (MSD), swiped, or manually entered:
  - If card in Credit BIN range:
    - If Debit enabled, and card was swiped, prompt for Credit or Debit
    - If Debit disabled, or card was tapped or manually entered, run as Credit
  - If Whitelist enabled, and card in Whitelist BIN range, run as Whitelist Gift
  - If card in specific (not all-inclusive) Gift BIN range, run as Heartland Gift
  - If card not in any of the above ranges, check all-inclusive ranges\* per the following table:

All-inclusive ranges*	Action
-----------------------	--------

Debit	EBT	Gift	
Disabled	Disabled	Disabled	Prompt "CARD NOT SUPPORTED"
<b>Enabled</b>	Disabled	Disabled	Run as Debit (if swiped)
Disabled	<b>Enabled</b>	Disabled	Run as EBT
Disabled	Disabled	<b>Enabled</b>	Run as HMS Gift
<b>Enabled</b>	<b>Enabled</b>	Disabled	Prompt for Debit (if swiped) or EBT
Disabled	<b>Enabled</b>	<b>Enabled</b>	Prompt for EBT or Gift
<b>Enabled</b>	<b>Enabled</b>	<b>Enabled</b>	Prompt for Debit (if swiped), EBT, or Gift

## 6.3. Tip Processing

HPA supports tip processing features such as tip assist and split tip to make it easier for cardholders to tip on the SIP device during the sale. This enables HPA to authorize the full amount of the transaction including the tip, as opposed to adjusting the tip later, which provides the best chargeback protection to the merchant for all forms of payment.

### 6.3.1. Tip Enablement

For non-Gift transactions, the TIP SUPPORT (**TIP**) parameter determines if tip processing is enabled as follows:

Value	Meaning
0 (OFF)	Tip processing is disabled for non-Gift transactions.  The <TipAdjustAllowed> element will be included in the sale response.
1 (PROMPT)	The SIP device will prompt for tip entry during a non-Gift sale.  If tip adjustment is allowed for the transaction, HPA will send <TipAdjustAllowed>1</TipAdjustAllowed> to the POS in the sale response, and the POS or SIP device may print a tip line on the receipt, e.g. in the event that the cardholder cancels/skips the tip prompt.

2 (PRINT)	<p>The SIP device will not prompt for tip entry during a non-Gift sale.</p> <p>If tip adjustment is allowed for the transaction, HPA will send <code>&lt;TipAdjustAllowed&gt;1&lt;/TipAdjustAllowed&gt;</code> to the POS in the sale response, and the POS or SIP device is expected to print a tip line on the receipt.</p>
-----------	---

For Gift transactions, the GIFT TIP SUPPORT (**GIFTTIP**) parameter determines if tip processing is enabled as follows:

Value	Meaning
0 (OFF)	<p>Tip processing is disabled for Gift transactions.</p> <p>The <code>&lt;TipAdjustAllowed&gt;</code> element will not be included in the sale response.</p>
1 (PROMPT)	<p>The SIP device will prompt for tip entry during a Gift sale.</p> <p>Since tip adjustment is not allowed for the Gift transaction, HPA will send <code>&lt;TipAdjustAllowed&gt;0&lt;/TipAdjustAllowed&gt;</code> to the POS in the sale response.</p>

### 6.3.2. Tip Prompting

Assuming the **TIP** parameter is set to 1 (PROMPT), the TIP ASSIST (**TIPASSIST**) and SPLIT TIP (**SPLITTIP**) parameters determine the type of tip prompting on the SIP device as follows:

TIPASSIST	SPLITTIP	Meaning
0 (OFF)	0 (OFF)	Basic prompt is displayed allowing the cardholder to enter a tip amount.
0 (OFF)	1 (ON)	Split tip prompt is displayed allowing the cardholder to split their tip between multiple servers/stylists.
1 (ON)	0 (OFF)	Tip assist prompt is displayed allowing the cardholder to choose between 3 suggested tip amounts or enter a tip amount.
1 (ON)	1 (ON)	Invalid configuration. TIPASSIST assumed to be 0 (OFF).

**NOTE:** Tip prompting only occurs during a sale transaction.

### 6.3.2.1. Add Tip Prompt

If the WANT TO TIP PROMPT (**WANTTOTIP**) parameter is set to 1 (ON), and the POS does not send a <TipAmount> element in the Sale request, the SIP device will prompt the cardholder as to whether or not they want to leave a tip.

**NOTE:** Add tip prompt only occurs when **TIP** parameter set to 1 (PROMPT).

Heartland	Heartland
<div>SALE: \$51.23</div> <div>WOULD YOU LIKE TO ADD A TIP?</div> <div> <div>YES</div> <div>NO</div> </div>	<div>SALE: \$51.23</div> <div>ADD TIP?</div> <div>1=YES</div> <div>2=NO</div>

If YES is selected, the SIP device will proceed with the appropriate tip entry prompt(s). If NO is selected, the SIP device will skip the tip entry prompt(s) and proceed as if a \$0 tip was entered.

### 6.3.2.2. Add Additional Tip Prompt

If the POS sends a <TipAmount> element in the Sale request containing a non-zero amount indicating that a tip amount has already been included in the sale amount (e.g. automatic gratuity added for a large party), the SIP device will prompt the cardholder as to whether or not they want to leave an additional tip.

If YES is selected, the SIP device will proceed with the basic tip prompt. If NO is selected, the SIP device will skip the tip entry prompt and proceed as if a \$0 tip was entered.

Heartland	Heartland
<div>SALE: \$51.23</div> <div>TIP INCLUDED: \$15.00</div> <div>ADD ADDITIONAL TIP?</div> <div> <div>YES</div> <div>NO</div> </div>	<div>SALE: \$51.23</div> <div>TIP INCLUDED: \$15.00</div> <div>ADD ADDITIONAL TIP?</div> <div>1=YES</div> <div>2=NO</div>

### 6.3.2.3. Basic Tip Prompt

The cardholder is prompted to enter a tip amount. A zero amount may be entered.



Heartland	Heartland
SALE: \$51.23 ENTER TIP AMOUNT  \$____.____	SALE: \$51.23 ENTER TIP AMOUNT  \$____.____

**NOTE:** If the cardholder presses the Cancel (X) or Enter (O) key at this screen, or a timeout occurs, HPA will proceed as if a \$0 tip was entered.

#### 6.3.2.4. Tip Assist Prompt

The cardholder is prompted to choose between 3 suggested tip amounts or select OTHER to enter a tip amount using the basic tip prompt. The 3 suggested amounts are driven by the percentages specified in parameters **TIPAST1**, **TIPAST2**, and **TIPAST3**. If those parameters are not specified, then default values of 10%, 15%, and 20% will be used respectively. Tip assist suggestions will be made based on the total amount of the sale, not the base amount.

**NOTE:** If any suggested tip amount would exceed \$9,999.99, the basic tip prompt will be used instead.

Heartland	Heartland				
SALE: \$51.23 SELECT TIP AMOUNT <table border="1"> <tr> <td>10% = \$5.12</td> <td>15% = \$7.68</td> </tr> <tr> <td>20% = \$10.25</td> <td>OTHER</td> </tr> </table>	10% = \$5.12	15% = \$7.68	20% = \$10.25	OTHER	SALE: \$51.23 SELECT TIP AMOUNT 1=10% \$5.12 2=15% \$7.68 3=20% \$10.25 4=OTHER
10% = \$5.12	15% = \$7.68				
20% = \$10.25	OTHER				

**NOTE:** If the cardholder presses the Cancel (X) or Enter (O) key at this screen, HPA will proceed as if a \$0 tip was entered.

#### 6.3.2.5. Split Tip Prompt

If the POS sends 2 or more <ServerLabel> elements in the Sale request, the cardholder is prompted to select whether they want to split the tip evenly across all servers/stylists, or enter a tip for each server/stylist.

Heartland	Heartland
SALE: \$51.23 SELECT TIP SPLIT	SALE: \$51.23 SELECT TIP SPLIT 1=EVENLY 2=INDIVIDUALLY
EVENLY   INDIVIDUALLY	

NOTE: If the cardholder presses the Cancel (X) or Enter (O) key at this screen, HPA will proceed as if a \$0 tip was entered.

If the cardholder decides to split the tip evenly, they will be prompted to enter the total tip amount using the basic prompt.

If they decide to enter a tip for each server/stylist, they will be prompted according to the <ServerLabel> elements sent in the Sale request.

For example, if the POS sent <ServerLabel>ENTER TIP AMOUNT FOR STYLIST AMANDA</ServerLabel> the prompt would appear as shown below. This prompt would be repeated for each <ServerLabel> specified by the POS. A zero amount may be entered.

If there is only one <ServerLabel> then SELECT TIP SPLIT screen will not be displayed, instead HPA will show the <ServerLabel> text on tip entry screen.

If the cardholder enters a tip amount for server such that the total tip amount in the transaction so far exceeds MAX\_TIP\_AMOUNT, then HPA will display a “TIP AMOUNT EXCEEDS LIMIT” error and will prompt again to get tip amount for all servers.

NOTE: If the POS does not send any <ServerLabel> elements, the basic tip prompt will be used.

Heartland	Heartland
SALE: \$51.23 ENTER TIP AMOUNT FOR STYLIST AMANDA	SALE: \$51.23 ENTER TIP AMOUNT FOR STYLIST AMANDA
\$____.____	\$____.____

**NOTE:** If the cardholder presses the Cancel (X) or Enter (O) key at this screen, HPA will proceed as if a \$0 tip was entered for the current server/stylist. HPA will then prompt tip for next server/stylist if there are any remaining, otherwise it will proceed with the transaction flow.

**NOTE:** Split Tip is currently only supported on the Lane/5000.

### 6.3.3. <TipAmount> Element

The <TipAmount> element has several uses:

- If the tip is entered/known on the POS prior to initiating the sale transaction, the POS can send a <TipAmount> element containing the tip amount in the Sale request and HPA will do no further tip processing.
- If the tip is prompted and entered/selected on the SIP device during the sale transaction, HPA will return a <TipAmount> element in the Sale response containing the tip amount.
- If the tip amount is not specified by the POS, or entered on the SIP device, and HPA returns <TipAdjustAllowed>1</TipAdjustAllowed> in the Sale response, the POS may print a tip line on the receipt. After the cardholder writes in their tip on the receipt, the POS can send a TipAdjust command with a <TipAmount> element to specify the tip amount to add to the previously authorized transaction.
- In SAF and Batch detail reports, the tip amount is provided in the <TipAmount> element.

### 6.3.4. <AdditionalTipAmount> Element

The <AdditionalTipAmount> element will contain additional tip amount entered on terminal for a Sale transaction with default tip included.

### 6.3.5. <TipAdjustAllowed> Element

This element is used to inform the POS whether tip adjustment is allowed for the transaction.

Element Value	Definition
0	Tip adjustment is not allowed for transaction. POS should not print a tip line on receipt.
1	Tip adjustment is allowed for transaction. POS may print a tip line on receipt.  <b>NOTE:</b> Tip adjustment is currently allowed for Credit Sale, CreditAuth, CreditOfflineSale and CreditOfflineAuth transactions.

### 6.3.6. TipAdjust Command

If `<TipAdjustAllowed>1</TipAdjustAllowed>` is returned to the POS in the sale response, this command may be used to add a tip to a previously approved transaction.

**NOTE:** The deprecated `CreditTipAdjust` command can also be used for tip adjustment, although it is recommended to use the `TipAdjust` command instead.

- Allows the merchant to alter the data on a previously approved `CreditSale`, `CreditAuth`, `CreditOfflineSale` or `CreditOfflineAuth` transaction.
- If tip is being adjusted for an online approved transaction, HPA uses the `ResponseId` to look up the details of previously approved transaction. HPA determines if the transaction is eligible for tip adjustment, and if so, updates the transaction with the tip and new total amount.

**NOTE:** The POS sends the `ResponseId` from the transaction for which the tip is being adjusted in the `<TransactionId>` element in the `AdjustTip` command.

- If tip is being adjusted for an offline approved transaction that is stored in the local transaction file (e.g. SAF, voice auth, or EMV offline approval), HPA updates the transaction with the tip and new total amount prior to submitting to the host.

**NOTE:** For a SAF transaction, the tip adjustment will be allowed even if the new total amount of the transaction including the tip exceeds the SAF limit specified by the `SAF AMOUNT MAX (STORFL)` parameter.

See [TipAdjust Command](#) for more details.

## 6.4. Cashback Processing

HPA supports cashback prompting for PIN Debit and EBT Cash Benefits transactions.

### 6.4.1. Cashback Enablement

The `DEBIT CASHBACK SUPPORT (CASHBACK)` parameter determines if cashback prompting is enabled for Debit as follows:

Value	Meaning
0 (OFF)	The SIP device will not prompt for PIN Debit cashback.

1 (ON)	<p>The SIP device will prompt for cashback for PIN Debit transactions.</p> <p><b>NOTE:</b> For contactless EMV PIN Debit, Mastercard requires that the cashback amount be provided to the card when it is tapped, so if the transaction has not been identified as a debit transaction prior to a Mastercard card being tapped, the SIP device will not prompt for cashback.</p>
--------	--

The EBT CASHBACK SUPPORT (**EBTCASHBACK**) parameter determines if cashback prompting is enabled for EBT Cash Benefits as follows:

Value	Meaning
0 (OFF)	The SIP device will not prompt for EBT Cash Benefits cashback.
1 (ON)	The SIP device will prompt for cashback for EBT Cash Benefits transactions.

#### 6.4.2. Cashback Prompting

Assuming the CASHBACK parameter is set to 1 (ON); the CASHBACK ASSIST (CBASSIST) parameter determines the type of Debit cashback prompting on the SIP device as follows:

Value	Meaning
0 (OFF)	Basic prompt is displayed allowing the cardholder to enter a cashback amount.
1 (ON)	Cashback assist prompt is displayed allowing the cardholder to choose between 3 suggested cashback amounts or enter a cashback amount.

##### 6.4.2.1. Basic Cashback Prompt

The cardholder is prompted to enter a cashback amount. A zero amount may be entered.

Heartland	Heartland
<p>SALE: \$51.23</p> <p>ENTER CASHBACK AMOUNT</p>	<p>SALE: \$51.23</p> <p>ENTER CASHBACK AMOUNT</p>

\$____.____	\$____.____
-------------	-------------

**NOTE:** If the cardholder presses the Cancel (X) or Enter (O) key at this screen, HPA will proceed as if \$0 cashback was entered.

#### 6.4.2.2. Cashback Assist Prompt

The cardholder is prompted to choose between 3 suggested cashback amounts or select OTHER to enter a cashback amount using the basic cashback prompt. The 3 suggested amounts are driven by the amounts (in cents) specified in parameters **CBAST1**, **CBAST2**, and **CBAST3**. Only the dollars will be displayed, not the cents. If those parameters are not specified, or any of them exceed the **CBLIMIT** parameter, then the basic cashback prompt will be used instead.

**NOTE:**

- The cashback assist prompt is only displayed for PIN Debit transactions, not EBT transactions. For EBT transactions, the basic cashback prompt will be displayed instead.

Heartland		Heartland
SALE: \$51.23 SELECT TIP AMOUNT		SALE: \$51.23 SELECT TIP AMOUNT
\$20	\$40	1=\$20 2=\$40 3=\$60 4=OTHER
\$60	OTHER	

**NOTE:** If the cardholder presses the Cancel (X) or Enter (O) key at this screen, HPA will proceed as if \$0 cashback was entered.

#### 6.4.3. Cashback Limit

If the cashback amount entered/selected by the cardholder exceeds the limit specified by the CASHBACK LIMIT (**CBLIMIT**) parameter, the SIP device will display a “CASHBACK AMOUNT EXCEEDS LIMIT” error and prompt for cashback again.

**NOTE:** The CBLIMIT parameter must be in the range of \$50.00 to \$200.00. If set lower than \$50.00, HPA will use \$50.00 as the limit. If set higher than \$200.00, HPA will use \$200.00 as the limit. This limit only applies to PIN Debit transactions, not EBT transactions.

#### 6.4.4. <CashbackAmount> Element

If the **CASHBACK** parameter is set to 1 (ON), the <CashbackAmount> element will be returned in all PIN Debit transaction responses. If the **EBTCASHBACK** parameter is set to 1 (ON), the <CashbackAmount> element will be returned in all EBT Cash Benefits transaction responses. It will either be set to the amount entered or selected by the cardholder, or set to 0 if the cardholder pressed the Cancel or Enter key at the cashback prompt.

If the sale is partially approved by the host, the cashback amount may be reduced or even zeroed out depending on the partially approved amount. When this occurs, the SIP device will display this information to the cardholder and allow them to accept or reject the partial approval. If accepted, the reduced amounts will be returned to the POS. If rejected, HPA will void the transaction and send a response to the POS accordingly.

## 6.5. Signature Capture

### 6.5.1. Signature Capture on SIP

Transaction signatures are captured with the following conditions:

- A signature capture screen will be prompted for following transactions if signature capture requirements are met irrespective of the card acquisition method.
  - Sale
  - Refund
  - Voice Authorization
- PIN verified transactions will not prompt for signature unless the Cardholder Verification Method for an EMV transaction calls for both PIN and Signature.
- For all EMV transactions, a signature screen will be prompted if the card CVM has a signature required method and the sale amount is above the signature limit.

### 6.5.2. Signature Data to Portico

- Once a signature is captured, it will be stored in the SIP device and will be sent to Portico on the next online transaction (piggy backed). See Piggy back section for more details.
- Captured signatures will be stored as a BMP file and sent to Portico in Base64 format.
- If required, captured signatures can be retrieved and verified on the Portico Gateway website. To view signatures on the website, please login to the Portico website with the appropriate site credentials and select the 'Transaction detail' radio button and provide the Gateway Transaction ID of the transaction for which you want to retrieve the signature.
- Signature data can be sent to Portico even after the transaction is batch closed, e.g. if the signature data is sent as part of EOD processing and the batch is previously auto closed at Portico before EOD.

### 6.5.3. Signature Data to POS

- HPA will send the signature data as a BMP in Base64 encoded format to POS in the transaction response. The data sent will always be 7016 bytes in length.
- POS can decode the Base64 data and display the signature as a BMP image.



## 6.6. Cancel Key Configuration

Customers can cancel the financial transaction by pressing the cancel key. The **CANCELKEY** parameter will define the default behavior of the cancel key at all screens displayed during a financial transaction flow.

Screen Type	Screen Behavior
Image	Ignore and Beep
Status	No Action
Choice	Cancel key will behave as per configuration of CANCELKEY
Input	Cancel key will behave as per configuration of CANCELKEY
Card Acquisition	Cancel key will behave as per configuration of CANCELKEY
Signature	Ignore and Beep
PIN	Cancel key will behave as per configuration of CANCELKEY
Line Item	Ignore and Beep

The parameter can be set to one of the following values:

Value	Meaning
1 (CANCEL)	If the cancel key is pressed at any screen before the transaction is sent to the gateway for authorization, cancel the transaction. If the cancel key is pressed at any screen after the transaction is approved, ignore and error beep.
2 (SKIP)	<p>If the cancel key is pressed and the screen can be skipped, skip the screen. If the cancel key is pressed and the screen cannot be skipped, ignore and beep. For example:</p> <ul style="list-style-type: none"> <li>• <b>Card Acquisition</b> - For card security code entry, skip and proceed with reason selection. For all other card acquisition related screens, ignore and error beep.</li> <li>• <b>Tip</b> - Skip tip selection/entry and proceed as if \$0 was entered.</li> <li>• <b>Cashback</b> - Skip cashback selection/entry and process as if \$0 was entered.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>PIN</b> - If Credit and PIN bypass is enabled, skip PIN entry and proceed with PIN bypass. If Debit or EBT or PIN bypass is disabled, ignore and error beep.</li> <li>• <b>Signature</b> - Ignore and error beep.</li> <li>• <b>Amount Confirmation</b> - Ignore and error beep.</li> </ul>
3 (IGNORE)	If the cancel key is pressed, ignore and error beep.

**NOTE:** During data entry, if the user has already entered some data, a cancel key press simply clears the entry, and only if there is no entry would the above logic be enacted.

## 6.7. Software Updates

If the PERFORM HEARTBEAT (**HRTBEAT**) parameter is enabled, HPA sends a daily Heartbeat message to HUDS after EOD processing to determine if a software update is available, and if it is then HPA automatically downloads the new software via a Differential download

**NOTE:** This Heartbeat does not update between major version releases.

However, it may be desirable for the merchant to have greater control over if and when to download new software and/or parameters, and they may do that by disabling Heartbeat and utilizing the Download command.

### 6.7.1. Heartbeat Disablement

The PERFORM HEARTBEAT (**HRTBEAT**) parameter determines if Heartbeat is enabled as follows:

Value	Meaning
0 (OFF)	Heartbeat is disabled. HPA will not send a Heartbeat message to HUDS after EOD processing.
1 (ON)	Heartbeat is enabled. HPA will send a Heartbeat message to the HUDS after EOD processing to check if a software update is available.

### 6.7.2. Download Command

The Download command is used to initiate a download of new HPA software and/or parameters from HUDS.

See [Download Command](#) for more details.

## 6.8. Power Management

**NOTE:** This section applies to portable devices only.

### 6.8.1. Sleep Mode

Portable terminals have the ability to go into sleep mode after a period of inactivity. The period of inactivity after which the device will go into sleep mode is configurable through the parameter **STNBYDELAY** (standby delay). This parameter can be set through WebTOPs or through terminal. The standby delay is specified in seconds.

- The valid values for STNBYDELAY parameter is from 20 (minimum value) to 9999 (maximum value) seconds. If STNBYDELAY parameter is given a value less than the minimum value (20 seconds), then the parameter is set to the minimum value. If STNBYDELAY parameter is given value greater than maximum value (9999 seconds), then the parameter is set to the maximum value. If STNBYDELAY parameter is set to 0, then sleep mode should be disabled.
- When the device is idle, it enters sleep mode until a new action is taken. The sleep mode timer is started once the device reaches the idle state. The device goes to sleep mode once the sleep mode timer is over.
- If a key is pressed on device or if a POS message is sent to the device when it is in the idle state, then the sleep mode timer will be restarted.
- The device will exit from sleep mode if any key on the device is pressed.
- The device should not go to sleep mode during payment processing.
- The device should not go to sleep mode during processing of pre or post custom payment form.
- The device should not go to sleep mode during infinite time screens. Example: LineItem or Signature.
- **NOTE:** Even when the **STNBYDELAY** parameter value is 20 seconds and idle timeout is 30 seconds (i.e. **STNBYDELAY** value is lesser than idle timeout), the device should not go to the sleep mode before it reaches the idle state. The sleep mode timer starts only when the device is in idle state.
- When the device wakes from sleep mode and if DHCP is used, there is a chance for the device IP to change. This is because if DHCP is used then there is no way to lock the device to the same IP address unless the DHCP server is configured via associating MAC addresses and their IP address. The other way for the device to stop to see its IP change is by setting the ethernet configuration to STATIC IP. And it is recommended to Merchants to keep standby delay a little higher to avoid frequent IP Changes on device.

### 6.8.2. Battery Level Indicator

For ISMP devices, the battery level indicator is displayed at the top right corner on a black strip.

Battery level indicator is represented by a small energy bar symbol and a numeric value to the right of the bar. The status of the battery bar indicates the device battery level and its corresponding numerical value is displayed on the right side of the battery bar. The energy level in the battery bar and its numerical value changes when the device battery level is changed.

The battery bar has six levels to indicate the device battery level. The level in the battery bar changes as the device battery level changes. When the device is charging, the battery bar displays a lightning bolt symbol in it.

The numerical value to indicate the device battery level and its value ranges from 0 to 100 %.

When the device is in idle mode, the battery level indicator is reflected for every idle timeout. But during active mode, the battery level indicator is reflected only at the beginning of displaying a screen.

Ex: If battery level changes from 74 to 75 % during card acquisition screen, the battery bar and numerical value will not be reflected immediately in the same card acquisition screen but will be reflected once the next screen is displayed.

### 6.8.3. Battery Level Warning

Portable terminals display a low battery warning [LOW BATTERY;CHARGE THE TERMINAL] if battery level drops below **BTRWRNGLVL** (7%). The default value of **BTRWRNGLVL** is 7%.

When the device is in idle mode, it continues to display a full screen warning message for every IDLETO (Idle Timeout). The full screen warning is prompted for **BTRWRNGTIME** (5 seconds).

When device battery is less than **BTRWRNGLVL**, wherever a standard HPA banner is displayed, it is replaced with a low battery banner.

**NOTE:** Since currently ISMP devices process SIPAdmin transaction in text mode, no warning will be displayed during this transaction.

Whenever the device wakes from sleep mode, it should prompt the full screen warning message.

When the device is charging (USB, charger or base) and even if the battery level is below **BTRWRNGLVL**, no full screen warning message or low battery banner will be displayed.

**NOTE:** The full screen battery warning depends on idle timeout. So if the promo image display is ON in the device, the full screen warning message will be prompted for every promo timeout and not on idle timeout. For ISMP devices (IMP650, IMP620) the promo image display is OFF by default.

## 6.9. Whitelist Processing

HPA provides the capability for the POS to support third party gift cards from various providers, by allowing the POS to process those transactions instead of HPA. A special whitelist file may be loaded onto HPA, which defines custom BIN ranges where HPA will send cleartext PAN and track data to the POS instead of attempting to authorize the transaction directly.

The following safeguards are in place to ensure that the overall system remains PCI compliant:

- Whitelist processing is only available for gift card sale, gift card balance inquiry, and gift add value transactions.
- The whitelist file is a signed file to ensure the security and integrity of the contents of the file.
- Whitelist processing is only performed if the WHITELIST parameter is enabled. This parameter is controlled by the Heartland WebTOPs system and is not configurable on the device.
- HPA compares the BIN ranges in the whitelist file with known BIN ranges of the four major credit cards to ensure that no credit card will be processed as a whitelisted card.

If the PAN of the swiped Gift card falls into a BIN range and PAN length range in the whitelist, and does not fall into any bank card BINs, HPA will not authorize the transaction, but rather will return the cleartext card data to the POS. The ResultText element is returned with “WHITELIST TRANSACTION”, and the CardAcquisition and TransactionTime elements are sent in the response.

## 6.10. Batch Retrieval

HPA provides an option “**BATCH RETRIEVAL**” in SIP ADMIN Menu to retrieve current batch file at any point of time. Using this facility, Current batch file can be copied to the shared drive on the SIP Device which can be very useful to fetch and execute transactions later if something went wrong on SIP Device due to a software or hardware failure.

Whenever the current batch file needs to be retrieved, Point of Sale can issue a ManagerMenu command to put the SIP device into the SIP Admin state. See [ManagerMenu Command](#).

After the SIP Device receives the ManagerMenu command it will prompt for the Admin password. Once the Admin password has been entered, the SIP Device will display a menu allowing the user to select among editing parameters, performing a download and batch retrieval.

Heartland	Heartland

SELECT FUNCTION		
EDIT PARAMETERS		
DOWNLOAD		
<=	BATCH RETRIEVAL	=>

SELECT FUNCTION  1=EDIT PARAMETERS 2=DOWNLOAD 3=BATCH RETRIEVAL  7=PREV      9=NEXT
---

If **BATCH RETRIEVAL** option is selected, SIP Device will save a copy of current batch file with '.BDX' file extension in shared drive and display the relevant message on SIP Device screen per below:

- "BATCH FILE COPIED TO SHARED DRIVE" if success.
- "ERROR COPYING BATCH FILE" if it fails to copy.
- "BATCH FILE NOT FOUND" if batch File is not available.

**NOTE:** Currently batch file can be deleted from host/shared drive via LLT only.

## 6.11. Ping Remote URL

HPA provides an option "PING URL" in SIP ADMIN Menu to ping a remote url which will help to troubleshoot network issues.

Whenever the network needs to be checked, Put the SIP device into the SIP Admin state. Within the admin menu, the SIP Device will display a list of options. Press "Next" to access "PING URL".

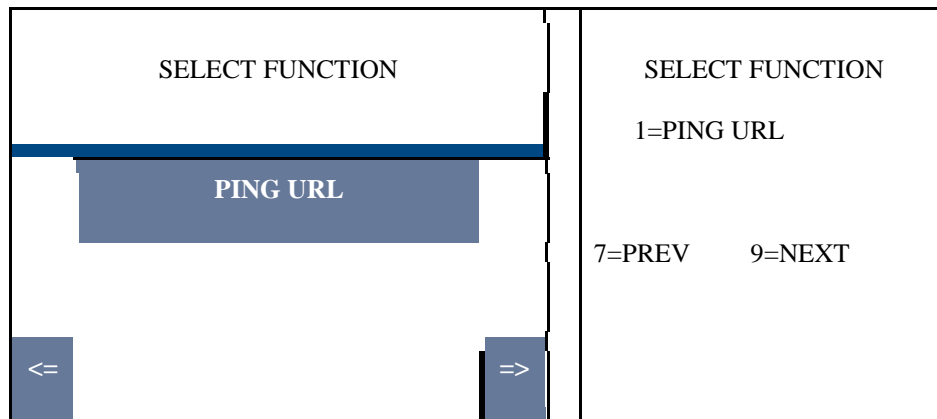
Heartland		
SELECT FUNCTION		
EDIT PARAMETERS		
DOWNLOAD		
<=	BATCH RETRIEVAL	=>

Heartland
SELECT FUNCTION  1=EDIT PARAMETERS 2=DOWNLOAD 3=BATCH RETRIEVAL  7=PREV      9=NEXT

Heartland		
-----------	--	--

Heartland		
-----------	--	--



If PING URL option is selected, SIP Device will ping the remote url and display the relevant message on SIP Device screen per below:

- “PINGING <RemoteURL>” while pinging. If <RemoteURL> is more than the max number of characters supported per line. <RemoteURL> will be truncated and replaced with “...” at the end of line.
- “PING SUCCESS” if SIP device is able to reach the remote url.
- “PING FAILED” if the SIP device is unable to reach the remote url.

HPA provides retry option after ping success or fail, the SIP device will display a choice allowing the user or select among “RETRY” and “EXIT”.

1. RETRY - SIP Device will ping the remote url again.

EXIT - SIP Device will come out from the ping url option.

## 7. User Interface

### 7.1. Common UI behavior

- If a key is pressed that is ignored by the application, there will be an audible beep but no screen flash.
- The CANCEL key will always cancel the transaction with a TRANSACTION CANCELLED message.
- Admin transactions cannot be cancelled by the user. They can only be interrupted by the POS.
- The CANCEL key is ignored on the signature capture screen. The POS can still cancel the transaction with a Reset command.
- If the POS cancels the transaction, a TRANSACTION CANCELLED message is displayed.
- If there is any error during a transaction or a function, UNABLE TO PROCESS message is displayed. An error code and error text is sent back to the POS so the POS can display it to the clerk.
- When any command is being processed, the first Reset command (sent typically when the POS wants to abort), displays TRANSACTION CANCELLED to let the user know that the current command is cancelled. It stays at this screen without any timeout. A second Reset command takes it to Lane Close/Open state.
- When a command is processed successfully (the transaction itself might be approved, declined or resulted in a processing error like a communications error, but the command is successfully processed), the result is displayed without any timeout. A Reset command takes it to Lane Close/Open state.
- At any user initiated error screen (i.e. an error as a result of user error), either pressing any key or a timeout will take the user back to the previous entry screen.
- Currently the following devices support graphical display.
  - Lane/3000
  - Lane/5000



## 7.2. Graphical Payment Flow

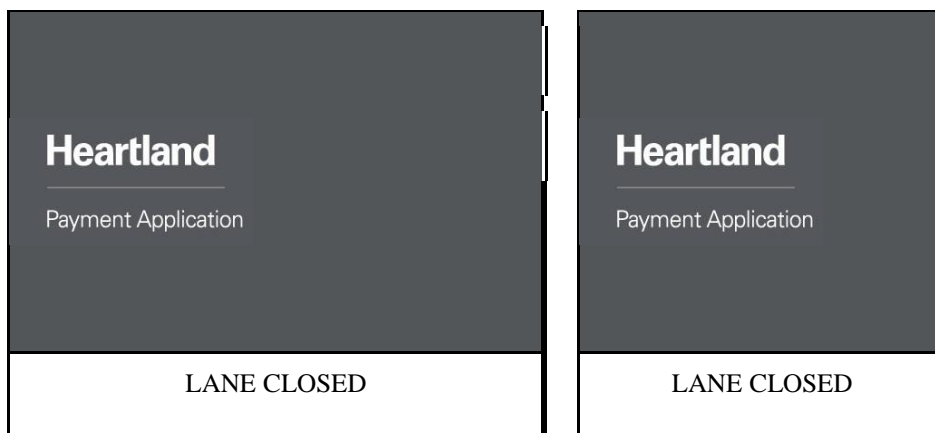
### 7.2.1. Overview

HPA supports a graphical mode by default if the SIP device supports it. During the payment flow, HPA uses the various graphical templates to display the payment screens.

### 7.2.2. Idle Logo

HPA displays an IDLELOGO.JPG image at Lane Closed and Lane Opened states. A default Heartland IDLELOGO.JPG is loaded from HUDS initially. This can be changed by the POS by sending a merchant specific IDLELOGO.JPG using the <SendFile> command. LANE CLOSED, LANE OPEN text is displayed on top of the IDLELOGO.JPG at the bottom.

- Lane/3000: IDLELOGO.JPG must be 320x240 resolution
- Lane/5000: IDLELOGO.JPG must be 480x320 resolution



### 7.2.3. Promotional Images

HPA displays promotional images instead of static Idle Logo at Lane Closed and Lane Opened states provided necessary settings were done using SetParameter command. To use promotional images, PromolImageDisplay parameter must be enabled. HPA can display up to 10 promotional images in loop at a predefined interval while SIP Device is in Lane Closed and Lane Opened states. All promotional images can be loaded in SIP device via SendFile Command.

The following parameters are used for Promotional Images on the SIP device:

- **PromolImage1 to PromolImage10:** Currently HPA has 10 promotional image parameters PromolImage1 to PromolImage10 to enable any image of supported format as promotional image. SIP Device would loop through these images at a predefined interval while the device is in Lane Closed and Lane Open states.

- **PromoImageDisplay:** PromoImageDisplay parameter must be enabled to display promotional images instead of static Idle Logo at Lane Closed and Lane Opened states.
- **PromoDisplayTime:** PromoDisplayTime parameter defines time interval for displaying each promotional image on the SIP Device. This parameter applies to all promotional images and is not set on a per-image basis.
- Promo image resolution:
  - Lane/3000: Must be 320 x 240
  - Lane/5000: Must be 480 x 320

## 7.2.4. Banner

### Banner Top Layout (UILAYOUT = 1)

HPA displays the BANNERXXX.JPG at all other payment screens. It is displayed at the top of each screen. It is a fixed sized banner leaving enough room for HPA to display its prompts.

- Lane/3000: BANNER320.JPG must be 320x40 resolution.



- Lane/5000: BANNER480.JPG must be 480x60 resolution.



### Banner Left Layout (UILAYOUT = 2)

HPA displays the BANNERXXXV.JPG at all other payment screens. It is displayed at the left of each screen. It is a fixed sized banner leaving enough room for HPA to display its prompts.

- Lane/3000: BANNER320V.JPG must be 240 x 32 resolution.



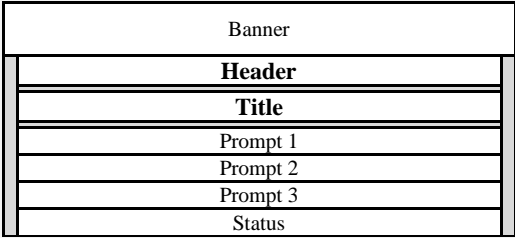
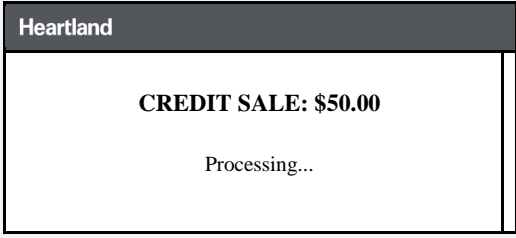
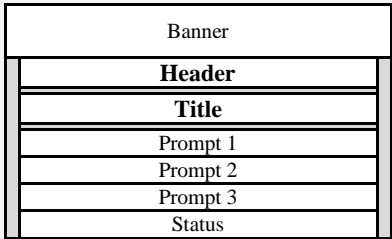
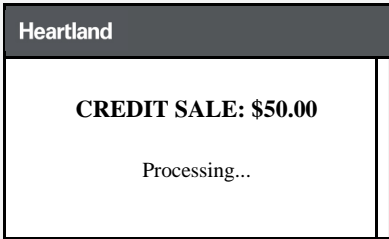
- Lane/5000: BANNER480V.JPG must be 320 x 48 resolution.



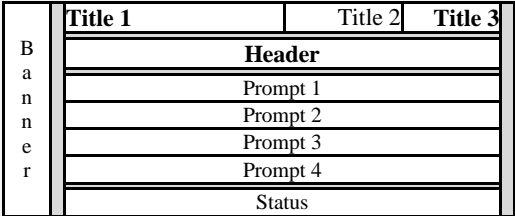
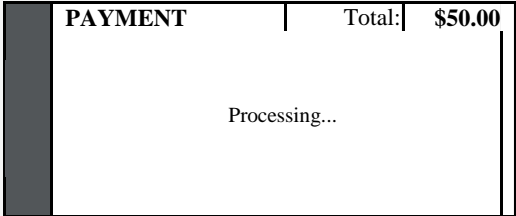
## 7.2.5. Status Screen

The status screen template contains only text. No buttons or edit boxes. Most of the screens in HPA use the status screen template. It is used to display some information to the user – during bootup, communications, displaying results, error text, etc.

### Banner Top Layout

Touch Screen	Example
	
Non-Touch Screen	Example
	

### Banner Left Layout

Touch Screen	Example
	

Non-Touch Screen	Example																															
<table><tr><td rowspan="8">B a n n e r</td><td>Title 1</td><td>Title 2</td><td>Title 3</td></tr><tr><td colspan="3">Header</td></tr><tr><td colspan="3">Prompt 1</td></tr><tr><td colspan="3">Prompt 2</td></tr><tr><td colspan="3">Prompt 3</td></tr><tr><td colspan="3">Prompt 4</td></tr><tr><td colspan="3">Status</td></tr><tr><td colspan="3"></td></tr></table>	B a n n e r	Title 1	Title 2	Title 3	Header			Prompt 1			Prompt 2			Prompt 3			Prompt 4			Status						<table><tr><td>PAYMENT</td><td>Total:</td><td>\$50.00</td></tr><tr><td colspan="3">Processing...</td></tr></table>	PAYMENT	Total:	\$50.00	Processing...		
B a n n e r		Title 1	Title 2	Title 3																												
		Header																														
		Prompt 1																														
		Prompt 2																														
		Prompt 3																														
		Prompt 4																														
		Status																														
PAYMENT	Total:	\$50.00																														
Processing...																																

### 7.2.6. Choice Screen

The choice screen template contains text and buttons. This screen is used to present a choice to the consumer so the consumer can select the choice (button). For example, on a card type selection, Yes/No screen, etc.

### 7.2.7. Edit Screen

The edit screen template contains text and one edit box. This screen is used to get data from the consumer. For example, a manual entry, CVV, Zip code, etc. The user enters the data using the physical keypad and should press ENTER when done.

Heartland	Heartland
SALE: \$12.34 ENTER TIP AMOUNT  \$____.____	SALE: \$12.34 ENTER TIP AMOUNT  \$____.____

## 7.3. GUI Customization

### 7.3.1. Color and Image Customization

The parameters under this section are used to customize the color of the prompt text, button text and button background, as well as displaying a custom background image throughout the transaction.

#### 7.3.1.1. BackgroundImage

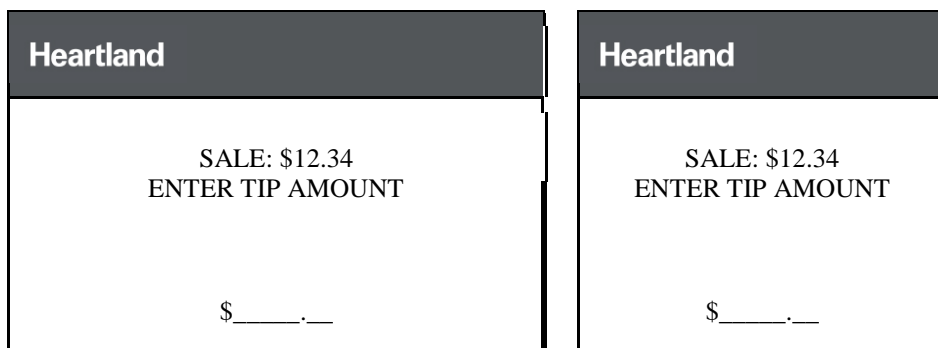
- Specifies the filename of the background image to be displayed on Lane Open screens.
- An image file should be loaded to the SIP device by using Send File command from the POS.
- Use the Set Parameter command to specify the filename of the loaded image. The SIP supports only .JPGs and the file extension is not case sensitive.

#### 7.3.1.2. PromptTextColor

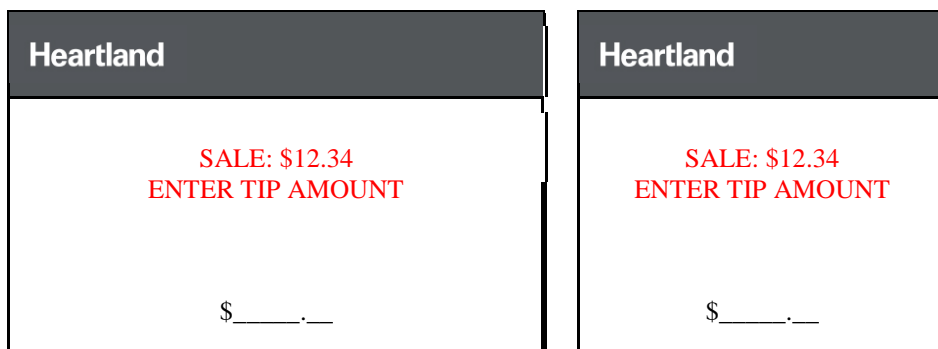
Used to set colors for prompts used in all screens.

- The desired color can be set using the Set Parameter command from the POS.
- Specified color can be any hexadecimal RGB value ranging from 000000 to FFFFFFFF.

The following image shows the default prompt text color in GUI devices.



The following images show the prompt text after setting the value of the parameter PromptTextColor to RED (FF0000).\_\_



#### 7.3.1.3. ButtonTextColor

Specifies the button text color on touch screen devices. Default color is white.

- The desired color can be set using the Set Parameter command from the POS.
- Specified color can be any hexadecimal RGB value ranging from 000000 to FFFFFFFF.
- Note: Applicable only for GUI touch screen devices like Lane/5000.

#### 7.3.1.4. ButtonBkgColor

Specifies the button background color on touch screen devices like Lane/5000. Default color is blue.

- The desired color can be set using the Set Parameter command from the POS.
- Specified color can be any hexadecimal RGB value ranging from 000000 to FFFFFFFF.

The following image shows the default button text color and background color on the touch screen device Lane/5000.

Heartland	
SELECT CARD TYPE	
CREDIT	DEBIT
EBT	GIFT

The following image shows the button text color and background color after the following changes are applied:

- ButtonTextColor set to Green (00FF00)
- ButtonBgColor set to Black (FFFFFF)

Heartland	
SELECT CARD TYPE	
CREDIT	DEBIT
EBT	GIFT

### 7.3.2. Promotional Images

The prompts under this section can be used to enable promotional images, upload the images, and set the time interval between the images to be displayed on the idle screen.

#### 7.3.2.1. PromolImageDisplay

Used to enable or disable the display of promotional images on the SIP.

It can be enabled or disabled using the Set Parameter command from the POS. Specify the value 1 to enable and 0 to disable.

#### 7.3.2.2. PromoDisplayTime

Specifies the time interval between the promotional images, if PromolImageDisplay is enabled.

- The time interval can be set using the Set Parameter command from the POS. Specify a value in seconds.



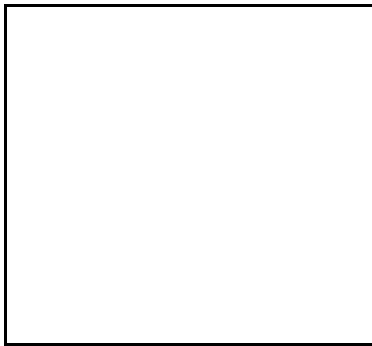
- If value is set to 0, it disables promotional images from being displayed irrespective of whether the PromolImageDisplay is enabled or not.

### 7.3.2.3. PromolImage1 to PromolImage10

Specifies the filename of the first promotional image to be cycled on idle screen.

- An image file should be loaded to the SIP device by using the Send File command from the POS.
- Use the Set Parameter command to specify the filename of the loaded image. The SIP device supports only .JPGs and the file extension is not case sensitive.

**NOTE:** The same applies for other promotional images i.e. PromolImage2 to PromolImage10.



## 7.4. Display Rules

- All text is centered, in all screens.
- Row1 and Row2 contain either a banner image.
- Row 3 contains:
- DO NOT REMOVE CARD or REMOVE CARD for EMV transactions where appropriate.
- Blank line where appropriate.
- Row 4 will always contain the Title - \* Transaction Type: \$12345.67 \* except for error screens. Error screens will contain the Title - \* Transaction Type \*
- Row 5, 6 contains status text
- Row 7 contains an Edit box (GUI) if user data input is needed.
- Row 7 contains buttons (GUI) if user selection is needed.
- Row 8 always contains the status messages (if any) or else a blank line.

### 7.4.1. Rules for displaying prompt lines

In HPA, there are three available prompt lines. The prompts should follow the below rules based on who will be seeing these prompts. This will be accomplished using the prompt file spreadsheet.

- Customer facing prompts
  - If one prompt is specified, it must be displayed on the second prompt line.
  - If two prompts are specified, they must be displayed on second and third prompt lines.
  - If three prompts are specified, they will be displayed on all three prompt lines.
- Non customer facing/System prompts
- Error and status update prompts will be displayed on the Status line.

## 7.5. SetKeys

### 7.5.1. Application settings

Application, say at bootup, can change the default settings of each template using DisplaySetKeys(). These settings are persistent until they are changed again.

Template	ENTER	CLEAR	CANCEL	TIMEOUT	NUMERIC (GUI Touch)	NUMERIC (GUI non-Touch, Text)
Menu	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled
Status	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled
Input	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled
Choice	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled
Navigation	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled

## 7.6. Custom Forms

- HPA supports custom GUI forms that a POS system can display before or after the payment flow to get user input. For example, to get a phone number, or to accept or decline some statement, etc.
- It is optional to use these forms and they do not affect the payment flow which is completely independent of these forms.
- POS cannot display these forms in the middle of the payment flow.

- For example, POS can display a couple of forms before payment, then perform the payment and then display a couple of post payment forms.
- It is completely up to the POS to control which forms, what order to display etc.
- Once a form is displayed, there is no timeout. HPA waits for the consumer action and returns the result to the POS. POS can always abort the form by sending a Reset command.
- Once the result is sent back to POS, the form continues to be displayed. It is up to the POS on the next steps – either display the next form, start payment or go back to Lane Open.
- Following table defines the custom form availability for different devices.

Feature	Touch devices	Non touch devices
StatusForm	Available	Available
ChoiceForm	Available	Available
EditForm	Available	Available
SignatureForm	Available	Not Available

### 7.6.1. Status Form

A typical use case is to infoRm something to the user.

- POS sends the text to display with one single button. The button text would also come from POS. <ButtonText> element is an optional tag. If sent, HPA displays the button with sent text, else button is not displayed. Note that if scrolling through the text is required and a button text is not provided by POS, HPA displays a default OK button.
- POS can send a maximum of 2000 characters and HPA will wrap the lines and display a scroll bar if needed. If more than 2000 characters are sent, HPA will truncate the message. No error will either be returned to POS or displayed on the terminal.
- If required, for touch devices, a scroll bar is provided. For non touch devices, PREV/NEXT buttons are displayed to scroll through the text. At the end, if a button text is sent from POS, it will be displayed, else a default OK button is displayed.

This form consists of a text field, and an optional button.

Heartland	Heartland
<FormText>	<FormText>
<ButtonText>	<ButtonText>

#### 7.6.1.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>StatusForm</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<FormText>	1-2000X	Mandatory	See <a href="#">&lt;FormText&gt;</a>
<ButtonText>	1-8X	Optional	See <a href="#">&lt;ButtonText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 7.6.1.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <Request>StatusForm</Request>
  <FormText>YOU EARNED 100 LOYALTY POINTS!</FormText>
  <ButtonText>OK</ButtonText>
</SIP>

```

Heartland	Heartland
YOUR EARNED 100 LOYALTY POINTS!	YOUR EARNED 100 LOYALTY POINTS

	OK	PRESS ANY KEY
--	----	---------------

### 7.6.1.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>StatusForm</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 7.6.1.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <SIPIId>15293SC80802518</SIPIId>
  <DeviceId>6194404</DeviceId>
  <Response>StatusForm</Response>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>SUCCESS</ResultText>
</SIP>

```

## 7.6.2. Choice Form

A typical use case is to get a simple choice from the consumer. For example, I Agree/Decline; Yes/No etc.

- POS sends the text to display with two buttons. The button text would also come from POS.

- POS can send a maximum of 2000 characters and HPA will wrap the lines and display a scroll bar if needed. If more than 2000 characters are sent, HPA will truncate the message. No error will either be returned to POS or displayed on the terminal.
- If required, for touch devices, a scroll bar is provided. For non-touch GUI devices, PREV/NEXT buttons are displayed to scroll through the text along with POS sent buttons.

This form consists of a text field and 2 buttons/choices.

Heartland	Heartland
<div style="text-align: center; padding: 10px;"> &lt;FormText&gt; </div> <div style="display: flex; justify-content: space-between; padding: 5px;"> <span>&lt;LeftButtonText&gt;</span> <span>&lt;RightButtonText&gt;</span> </div>	<div style="text-align: center; padding: 10px;"> &lt;FormText&gt; </div> <div style="padding: 5px;"> 1=&lt;LeftButtonText&gt;  2=&lt;RightButtonText&gt; </div> <div style="padding: 5px;"> 7=PREV      9=NEXT </div>

### 7.6.2.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>ChoiceForm</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<FormText>	1-2000X	Mandatory	See <a href="#">&lt;FormText&gt;</a>
<LeftButtonText>	1-8X	Mandatory	See <a href="#">&lt;LeftButtonText&gt;</a>
<RightButtonText>	1-8X	Mandatory	See <a href="#">&lt;RightButtonText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 7.6.2.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <Request>ChoiceForm</Request>
  <FormText>DO YOU WANT TO REDEEM LOYALTY POINTS TODAY?</FormText>
  <LeftButtonText>YES</LeftButtonText>
  <RightButtonText>NO</RightButtonText>
</SIP>

```

Heartland	Heartland
<p>DO YOU WANT TO REDEEM LOYALTY POINTS TODAY?</p> <p>YES   NO</p>	<p>DO YOU WANT TO REDEEM LOYALTY POINTS TODAY?</p> <p>1=YES 2=NO</p>

### 7.6.2.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>ChoiceForm</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<ChoiceSelected>	1-16X	Mandatory	See <ChoiceSelected>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

### 7.6.2.4. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <SIPIId>[SIP ID]</SIPIId>
  <DeviceId>[DEVICE ID]</DeviceId>
  <Response>ChoiceForm</Response>

```



```

<MultipleMessage>0</MultipleMessage>
<Result>0</Result>
<ResultText>SUCCESS</ResultText>
<ChoiceSelected>YES</ChoiceSelected>
</SIP>

```

### 7.6.3. Edit Form

A typical use case is to get customer information like date of birth, phone number, zip code etc.

- POS sends the text to display with one edit box. The text to display should be defined in 'CUSTOM.TXT' file. If POS sends any text other than defined in Custom.txt, HPA returns an error.
- The format of the edit box comes from the POS. The format rules are defined below.
- For alphanumeric data entry, it is required to click on edit box to launch virtual keypad for alphanumeric entries. A virtual keypad is displayed below the Edit Box for easy data entry. For numeric entries, the virtual keypad is disabled requiring use of the physical keypad with character support limited to those displayed on the keys. As such, "@" is not available for email addresses.
- HPA will not do any customer data entry validations before sending it to POS.

This form consists of a text field, and an edit box for entering data.

Heartland	Heartland
<FormText>	<FormText>
<EditBoxFormat>	<EditBoxFormat>

#### 7.6.3.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>EditForm</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>

<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<FormText>	1-2000X	Mandatory	See <a href="#">&lt;FormText&gt;</a>
<EditBoxFormat>	1-32X	Mandatory	See <a href="#">&lt;EditBoxFormat&gt;</a>
<EntryMask>	1N	Not supported	
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 7.6.3.2. <FormText>

The <FormText> element in an Edit Form may only contain one of the following:

- ENTER DATE OF BIRTH
- ENTER SOCIAL SECURITY NUMBER
- ENTER EMAIL ADDRESS
- ENTER AGE
- ENTER LOYALTY NUMBER
- ENTER REWARD NUMBER
- ENTER DRIVERS LICENSE NUMBER
- ENTER DRIVERS ID
- ENTER ODOMETER
- ENTER STREET ADDRESS
- ENTER CITY
- ENTER STATE
- ENTER ZIP CODE
- ENTER PHONE NUMBER

**NOTE:** If any other text is specified, HPA will respond with an “INVALID FORM TEXT” result.

#### 7.6.3.3. <EditBoxFormat>

- X for alpha-numeric
- N for numeric
- Any other character will be displayed as is in the edit box and skipped for entry.
- No error checking is done on the format string
- Max length is 32 characters including the format characters

Examples:

Element Value	Data Entry Type
---------------	-----------------

NNN-NNN-NNNN	Social Security Number
(NNN) NNN-NNNN	Phone Number
NNNNN	5-Digit Zip Code
NNNNN-NNNN	9-Digit Zip+4 Code
NN/NN/NNNN	Date of Birth

#### 7.6.3.4. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <Request>EditForm</Request>
  <FormText>ENTER PHONE NUMBER</FormText>
  <EditBoxFormat>(NNN) NNN-NNNN</EditBoxFormat>
</SIP>

```

Heartland	Heartland
<div>ENTER PHONE NUMBER</div> <div>( ) - </div>	<div>ENTER PHONE NUMBER</div> <div>( ) - </div>

#### 7.6.3.5. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPIId>	1-20X	Mandatory	See <a href="#">&lt;SIPIId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>

<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>EditForm</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<DataEntered>	1-32X	Mandatory	See <a href="#">&lt;DataEntered&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 7.6.3.6. Response Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <SIPId>[SIP ID]</SIPId>
  <DeviceId>[DEVICE ID]</DeviceId>
  <Response>EditForm</Response>
  <Result>0</Result>
  <ResultText>SUCCESS</ResultText>
  <DataEntered>4692947000</DataEntered>
</SIP>

```

#### 7.6.4. Signature Form

- POS sends form text to display with signature widget. The form text to display should be defined in 'CUSTOM.TXT' file. It's a signed file with allowed prompts. If POS sends any text other than defined in Custom.txt, HPA returns an error.
- HPA will capture the signature and returns base64 encoded signature data in BMP file format to POS as <AttachmentData>.

This form consists of a text field, and a signature box.

<b>Heartland</b>
<FormText>

CLEAR	ENTER
-------	-------

#### 7.6.4.1. Request Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>
<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<Request>	<b>SignatureForm</b>	Mandatory	See <a href="#">&lt;Request&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<FormText>	1-2000X	Mandatory	See <a href="#">&lt;FormText&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 7.6.4.2. Request Example

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <Request>SignatureForm</Request>
  <FormText>PLEASE SIGN YOUR NAME</FormText>
</SIP>

```

<b>Heartland</b>		
PLEASE SIGN YOUR NAME		
<b>John Doe</b>		
<table border="1"> <tr> <td>CLEAR</td> <td>ENTER</td> </tr> </table>	CLEAR	ENTER
CLEAR	ENTER	

#### 7.6.4.3. Response Schema

XML Element	Value	Usage	Description
<SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

<Version>	1-2N.N	Mandatory	See <a href="#">&lt;Version&gt;</a>
<ECRId>	1-20N	Mandatory	See <a href="#">&lt;ECRId&gt;</a>
<SIPId>	1-20X	Mandatory	See <a href="#">&lt;SIPId&gt;</a>
<DeviceId>	1-8N	Mandatory	See <a href="#">&lt;DeviceId&gt;</a>
<RequestId>	1-12N	Mandatory	See <a href="#">&lt;RequestId&gt;</a>
<Response>	<b>SignatureForm</b>	Mandatory	See <a href="#">&lt;Response&gt;</a>
<MultipleMessage>	1N	Mandatory	See <a href="#">&lt;MultipleMessage&gt;</a>
<Result>	1-4N	Mandatory	See <a href="#">&lt;Result&gt;</a>
<ResultText>	1-32X	Mandatory	See <a href="#">&lt;ResultText&gt;</a>
<AttachmentData>	var.	Mandatory	See <a href="#">&lt;AttachmentData&gt;</a>
</SIP>	--	Mandatory	See <a href="#">&lt;SIP&gt;</a>

#### 7.6.4.4. Response

```

<SIP>
  <Version>1.0</Version>
  <ECRId>[ECR ID]</ECRId>
  <SIPId>[SIP ID]</SIPId>
  <DeviceId>[DEVICE ID]</DeviceId>
  <Response>SignatureForm</Response>
  <MultipleMessage>0</MultipleMessage>
  <Result>0</Result>
  <ResultText>SUCCESS</ResultText>
  <AttachmentData>[SignatureData]</AttachmentData>
</SIP>

```

## 7.7. Error Messages

### 7.7.1. Transaction Canceled

- If a transaction is canceled by a Reset command from POS, HPA will display “TRANSACTION CANCELED” on the SIP device.

### 7.7.2. HPA Error

- If a transaction cannot be processed due to HPA not able to perform its job (e.g. communication error, etc.), HPA will display “UNABLE TO PROCESS” on the SIP device.

- A more detailed error is sent back to POS for reporting.

### 7.7.3. User Error

- If an error occurs due to consumer action, HPA will display the following error messages to let the consumer correct it and continue with the transaction.

Error Text	Why?	What to do?
PLEASE HOLD CARD OR PHONE TO READER UNTIL BEEP	If an EMV or MSD contactless card is tapped and the read fails	Re-tap closer and/or with a different orientation of the card
MULTIPLE CARDS DETECTED TAP ONE CARD ONLY	If multiple EMV or MSD contactless card reads are detected	Make you are tapping only one card Take card out of the wallet

## 7.8. Quick Access Screen

Quick Access Screen in HPA can be accessed while SIP device on idle screen by pressing 8, then 9, then ENTER. The user can see the HPA version and POS communication settings.

HPA provides an option to select “ADMIN MENU” on the Quick Access Screen. This allows the Administrative settings to be accessed without a POS command to update the setting while POS and SIP communications are down.

#### IP/Ethernet Mode:

Heartland	Heartland
vX.X.X.XXXXXXXXXX	vX.X.X.XXXXXXXXXX
IP: NNN.NNN.NNN.NNN	IP: NNN.NNN.NNN.NNN
PORT: NNNNN	PORT: NNNNN
ADMIN MENU	1=ADMIN MENU

#### Serial Mode:

Heartland	Heartland
-----------	-----------

vX.X.X.XXXXXXXXXX  PORT: [PORT] CONF: [FORMAT], [BAUD]	vX.X.X.XXXXXXXXXX  PORT: [PORT] CONF: [FORMAT],[BAUD]
<div>ADMIN MENU</div>	1=ADMIN MENU

- **PORT:** USB, RS232 RJ12, or RS232 DB9
- **FORMAT:** 7E1, 7N1, 7O1, 8E1, 8N1 or 8O1
- **BAUD:** 1200, 2400, 9600, 19200, 38400 or 115200



## 8. Parameters

### 8.1. Overview

Parameters affect the application's flow and behavior and are settings that are persistent across power loss.

Parameters are divided into sections. Each section is accessible from a specific menu selection and prints on the parameter report in a specific section. The order of items in the individual sections should match the order they are printed and displayed.

Binary Parameter Options: All Binary parameters provide these same options.

Display	Value
1=ON	1
2=OFF	0

Parameters are driven by WebTOPs and it is assumed that all non T (see below) parameters are always downloaded and WebTOPs or deployment does not rely on the default parameter values in the application. WebTOPs is the Heartland SIP device boarding tool used to configure parameters for a specific merchant.

The parameter tables contain the following information:

Column	Description
Parm Name	This value is used by HUDS to uniquely identify each parameter. The parameter names will be bolded throughout this document.
Description	The user friendly name of the parameter that is included in the parameter report and used in the Edit Parameters function.
View / Print?	This column indicates if a parameter is viewable from the Edit Parameters function. Some parameters can be viewed/printed but not edited.
Edit?	This column indicates where this parameter is editable. <ul style="list-style-type: none"> <li>W = WebTOPs only. Editable at WebTOPs only and cannot be edited at the SIP device. Downloaded to the SIP device. These are merchant specific</li> </ul>

	<p>parameters that are setup / edited at WebTOPs. If a merchant wants to change this parameter they need to call HSC and edit it via WebTOPs.</p> <ul style="list-style-type: none"> <li>• T = Terminal only. Editable at SIP device only and cannot be edited at WebTOPs. Not downloaded to the SIP device. These are location specific parameters that Heartland cannot control.</li> <li>• H = Hard-coded at WebTOPs. Not editable at WebTOPs or at the SIP device. Downloaded to the SIP device. These are application specific parameters that are the same across all merchants.</li> <li>• B = Both. Editable (or Hardcoded) at WebTOPs and at the SIP device. Downloaded to the SIP device.</li> </ul>
Edit Reboot?	This column indicates if a reboot of the SIP device is triggered after changing the setting.
Type	<p>This below describes possible values in the “Type” column of the parameters table. The length follows the type symbol, and is either an absolute length (e.g. B1) or allowed range (e.g. X0-42).</p> <ul style="list-style-type: none"> <li>• N = Numeric data only: 0-9</li> <li>• X = Alphanumeric: all alphabetic, numeric, and special characters</li> <li>• B = Boolean: only 0 (Off) and 1 (On) are allowed</li> </ul>
Default	This column refers to the parameter value that is typically used at deployment. The application is intended to always have the parameter set by Web Tops so this column is advisory and is not intended to indicate settings managed within the software.

## 8.2. Communication Parameters

This section contains settings used to configure the application for IP communications with the host.

Parm Name	Description	View/ Print?	Edit?	Edit Reboot?	Type	Default
-----------	-------------	-----------------	-------	--------------	------	---------

POSLNKTYPE	<div>POS LINK TYPE</div> <div>This parameter decides which interface is used for IP communication.</div> <table><tr><th>Display</th><th>Value</th></tr><tr><td>1=SERIAL</td><td>1</td></tr><tr><td>2=ETHERNET</td><td>2</td></tr><tr><td>3=WIFI</td><td>3</td></tr></table>	Display	Value	1=SERIAL	1	2=ETHERNET	2	3=WIFI	3	NO	H	YES	N1	As downloaded from WebTOPs						
Display	Value																			
1=SERIAL	1																			
2=ETHERNET	2																			
3=WIFI	3																			
IPCONNTYPE	<div>IP CONNECT TYPE</div> <div>This parameter decides which interface is used for IP communication</div> <table><tr><th>Display</th><th>Value</th></tr><tr><td>1=ETHERNET</td><td>1</td></tr><tr><td>2=Wi-Fi</td><td>2</td></tr><tr><td>3= GPRS</td><td>3</td></tr><tr><td>4=CDMA</td><td>4</td></tr><tr><td>5=CDMA 2</td><td>5</td></tr><tr><td>6=CDMA 3</td><td>6</td></tr></table>	Display	Value	1=ETHERNET	1	2=Wi-Fi	2	3= GPRS	3	4=CDMA	4	5=CDMA 2	5	6=CDMA 3	6	YES	B	NO	N1	As downloaded from WebTOPs
Display	Value																			
1=ETHERNET	1																			
2=Wi-Fi	2																			
3= GPRS	3																			
4=CDMA	4																			
5=CDMA 2	5																			
6=CDMA 3	6																			
LICENSEID	<div>LICENSE ID</div> <div>License ID used as part of login credentials to login to Portico</div>	YES	B	NO	X20	As downloaded from WebTOPs														

SITEID	SITE ID Site ID used as part of login credentials to login to Portico	YES	B	NO	X20	As downloaded from WebTOPs
DEVICEID	DEVICE ID Device ID used as part of login credentials to login to Portico	YES	B	NO	X20	As downloaded from WebTOPs
USERNAME	USER NAME User Name used as part of login credentials to login to Portico	YES	B	NO	X100	As downloaded from WebTOPs
PSW	PASSWORD Password used as part of login credentials to login to Portico	YES	B	NO	X100	As downloaded from WebTOPs
DEVELOPERID	DEVELOPER ID Developer ID used as part of login credentials to login to Portico	YES	B	NO	X6	As downloaded from WebTOPs
UDID	UNIQUE DEVICE ID Unique Device ID used as part of login credentials to login to Portico	YES	B	NO	X4	As downloaded from WebTOPs
SOAPURL	SOAP URL <a href="http://www.w3.org/2003/05/soap-envelope">http://www.w3.org/2003/05/soap-envelope</a>	YES	B	NO	X128	As downloaded from WebTOPs
GATEWAYURL	GATEWAY URL <a href="http://Hps.Exchange.Posgateway">http://Hps.Exchange.Posgateway</a>	YES	B	NO	X128	As downloaded from WebTOPs

PRIMARYWSURL	PRIMARY WS URL http://Hps.Exchange.Posgateway/PosGatewayService.asmx	YES	B	NO	X128	As downloaded from WebTOPs						
SECONDARYWSURL	SECONDARY WS URL http://Hps.Exchange.Posgateway/PosGatewayService.asmx	YES	B	NO	X128	As downloaded from WebTOPs						
PRIMARYURL	PORTICO PRIMARY URL posgateway.cert.secureexchange.net	YES	B	NO	X128	As downloaded from WebTOPs						
SECONDARYURL	PORTICO SECONDARY URL posgateway.cert.secureexchange.net	YES	B	NO	X128	As downloaded from WebTOPs						
PRIMARYPORT	PORTICO PRIMARY PORT 443	YES	B	NO	N6	As downloaded from WebTOPs						
SECONDARYPORT	PORTICO SECONDARY PORT 443	YES	B	NO	N6	As downloaded from WebTOPs						
STARTURL	START HOST URL Denotes application's preferred URL to start with for the next transaction. <table><tr><th>Display</th><th>Value</th></tr><tr><td>1=PRIMARY URL</td><td>1</td></tr><tr><td>2=SECONDARY URL</td><td>2</td></tr></table>	Display	Value	1=PRIMARY URL	1	2=SECONDARY URL	2	YES	N	NO	N1	1 (Primary URL)
Display	Value											
1=PRIMARY URL	1											
2=SECONDARY URL	2											

## 8.3. Display/Prompt Parameters

This section contains settings related to customizing the display and prompts in the application.

Parm Name	Description	View/ Print?	Edit?	Edit Reboot?	Type	Default
IDLETO	IDLE TIMEOUT Number of seconds of inactivity at a prompt before the SIP device times out and returns to idle. A value of 0 is replaced with 30 seconds.	YES	B	NO	N1-3	As downloaded from WebTOPs
BEEP	KEY BEEP Determines if keys beep whenever they are pressed. See Binary Parameter Options in Parameters Overview.	YES	B	YES	B1	As downloaded from WebTOPs
RESULTBEEP	RESULT BEEP Determines if invalid or Success keys beep whenever they are pressed. See Binary Parameter Options in Parameters Overview.	YES	B	YES	B1	As downloaded from WebTOPs
BEEPVOL	BEEPER VOLUME Controls loudness of beep on the SIP device.	YES	B	NO	N1-3	As downloaded from WebTOPs
MAFTO	MULTI-APP TIMEOUT Number of seconds of inactivity at the Idle menu before the SIP device times out and return to the MAF menu. A value of 0 indicates no timeout. A non-zero value is required for auto close to operate reliably.	YES	B	NO	N1-5	As downloaded from WebTOPs

BNNRTEXT1	BANNER TEXT 1 Text to display instead of Logo and Banner images in text mode. Note to set the value to blank, set to " " (double quote space double quote) in HUDS.	YES	H	NO	X0-21	As downloaded from WebTOPs
BNNRTEXT2	BANNER TEXT 2 Text to display instead of Logo and Banner images in text mode. Note to set the value to blank, set to " " (double quote space double quote) in HUDS.	YES	H	NO	X0-21	As downloaded from WebTOPs
TRMLMODEL	TERMINAL MODEL	NO	H	NO	X6	As downloaded from WebTOPs
SUPLANGS	SUPPORTED LANGUAGES List of all the languages supported by the terminal and used for display	NO	W	NO	X3	As downloaded from WebTOPs
DEFLANG	DEFAULT LANGUAGE The default language used the terminal for display	NO	W	YES	X3	As downloaded from WebTOPs
LOPENTEXT	LANE OPEN TEXT Text to display in text mode at idle when lane is open. Note to set to blank set to " " (double quote space double quote) in HUDS.	YES	B	NO	X0-21	As downloaded from WebTOPs
LCLOSETEXT	LANE CLOSED TEXT Text to display in text mode at idle when lane is closed. Note to set to blank set to " " (double quote space double quote) in HUDS.	YES	B	NO	X0-21	As downloaded from WebTOPs
PromptTextColor	PROMPT TEXT COLOR Specifies the prompt text color to be used on all screens on GUI	YES	W	NO	X6	000000

	<p>devices. If not specified, the default black prompt text will be used.</p> <p>Color should be specified in RGB hexadecimal format (e.g. FFFFFFFF).</p> <p>This color does not apply to LOPENTEXT and LCLOSETEXT.</p>					
PromoImageDisplay	<p>PROMO IMAGE DISPLAY</p> <p>If enabled, the promotional images specified by PromoImage1 - PromoImage10 and loaded to the device via the <a href="#">SendFile</a> command will be cycled on the idle screen at the time interval specified by PromoDisplayTime.</p>	YES	W	NO	B1	0 (OFF)
PromoDisplayTime	<p>PROMO DISPLAY TIME</p> <p>Specifies the time interval in seconds to display each promotional image.</p> <p><b>NOTE:</b> Setting this parameter to zero (0) will disable promotional image display.</p>	YES	W	NO	N1-3	5
PromoImage1	<p>PROMO IMAGE 1</p> <p>Specifies the filename of the first promotional image to be cycled on the idle screen.</p> <p>Must be in XXXXXXXX.JPG format and loaded to the device via the <a href="#">SendFile</a> command.</p>	YES	W	NO	X0-14	NULL
PromoImage2	<p>PROMO IMAGE 2</p> <p>Specifies the filename of the second promotional image to be cycled on the idle screen.</p>	YES	W	NO	X0-14	NULL



PromoImage3	PROMO IMAGE 3 Specifies the filename of the third promotional image to be cycled on the idle screen.	YES	W	NO	X0-14	NULL
PromoImage4	PROMO IMAGE 4 Specifies the filename of the fourth promotional image to be cycled on the idle screen.	YES	W	NO	X0-14	NULL
PromoImage5	PROMO IMAGE 5 Specifies the filename of the fifth promotional image to be cycled on the idle screen.	YES	W	NO	X0-14	NULL
PromoImage6	PROMO IMAGE 6 Specifies the filename of the sixth promotional image to be cycled on the idle screen.	YES	W	NO	X0-14	NULL
PromoImage7	PROMO IMAGE 7 Specifies the filename of the seventh promotional image to be cycled on the idle screen.	YES	W	NO	X0-14	NULL
PromoImage8	PROMO IMAGE 8 Specifies the filename of the eighth promotional image to be cycled on the idle screen.	YES	W	NO	X0-14	NULL
PromoImage9	PROMO IMAGE 9 Specifies the filename of the ninth promotional image to be cycled on the idle screen.	YES	W	NO	X0-14	NULL
PromoImage10	PROMO IMAGE 10 Specifies the filename of the tenth promotional image to be cycled on the idle screen.	YES	W	NO	X0-14	NULL
ButtonBkgColor	BUTTON BACKGROUND COLOR Specifies the button background color to be used on all buttons on	YES	W	NO	X6	1E90FF

	touchscreen devices. If not specified, the default blue buttons will be used.  Color must be specified in RGB hexadecimal format (e.g. FFFFFFFF).					
ButtonTextColor	BUTTON TEXT COLOR Specifies the button text color to be used on all buttons on touchscreen devices. If not specified, the default white button text will be used.  Color must be specified in RGB hexadecimal format (e.g. FFFFFFFF).	YES	W	NO	X6	FFFFFF
BackgroundImage	BACKGROUND IMAGE Specifies the filename of the background image to be displayed on all Lane Open screens.  Must be in XXXXXXXX.JPG format and loaded to the device via the <a href="#">SendFile</a> command.	YES	W	NO	X0-14	NULL
PartialAuthConfirm	PARTIAL AUTH CONFIRM Indicates if customer should be prompted to accept or decline a partially approved transaction.	YES	T	NO	B1	1

## 8.4. Download Parameters

This section contains settings related to downloading an Ingenico SIP device application from HUDS.

Parm Name	Description	View/ Print?	Edit?	Edit Re bo ot?	Type	Default
DLAPPID	DOWNLOAD SOFTWARE ID	YES	B	NO	X0-20	As downloaded

	Identifies the Software ID to the download system.					from WebTOPs
DLTERMID	DOWNLOAD TERMINAL ID Identifies the Terminal ID to the download system.	YES	B	NO	X1-8	As downloaded from WebTOPs
DLHOSTURL	DOWNLOAD HOST URL URL for communicating with download system for IP downloads.	YES	B	NO	X0-128	As downloaded from WebTOPs
DLPORT	DOWNLOAD HOST PORT Port for communicating with download system for IP downloads.	YES	B	NO	N1-5	As downloaded from WebTOPs
HRTBEAT	PERFORM HEARTBEAT Determines if heartbeat will be performed after each batch close or not.	YES	H	NO	B1	As downloaded from WebTOPs
HBERRORS	HEARTBEAT ERRORS Determines if communication errors will be displayed during a heartbeat. See Binary Parameter Options in Parameters Overview. NOTE: Defaulted to off to avoid helpdesk calls. To be turned on to troubleshoot heartbeat problems only.	YES	T	NO	B1	0
HBSKIP	HEARTBEAT SKIP DAYS Skips to Nth day for the heartbeat. Some examples: 0 = Don't skip at all. 1 = Skip to the next day. 2 = Skip to the 2nd day ...and so on 7 = Skip to the 7th day i.e. Skips 6 days. ...and so on	YES	B	NO	N1-3	As downloaded from WebTOPs
HBSKIPCOM	HEARTBEAT SKIP COMM Indicates on which comm. type the heartbeat should be skipped.	YES	H	NO	N1	As downloaded from WebTOPs

Display	Value	Meaning
1=DIAL	1	Skip on Dial only
2=IP	2	Skip on IP only
3=BOTH	3	Skip on both Dial and IP

## 8.5. Merchant Parameters

This section contains identifiers and application configuration options that are specific to the merchant.

Parm Name	Description	View/ Print?	Edit?	Edit Reboot?	Type	Default						
AQBIN	ACQUIRER BIN Identifies the merchant bank that signed the merchant who is using the POS application. This field is used in transactions.	YES	H	NO	N6	As downloaded from WebTOPs						
APPMODE	APPLICATION MODE <table><tr><th>Display</th><th>Value</th></tr><tr><td>1=RETAIL</td><td>0</td></tr><tr><td>2=RESTAURANT</td><td>1</td></tr></table>	Display	Value	1=RETAIL	0	2=RESTAURANT	1	YES	H	YES	N1	As downloaded from WebTOPs
Display	Value											
1=RETAIL	0											
2=RESTAURANT	1											
CURCD	CURRENCY CODE Identifies the merchant's authorization currency. 840 = United States. This field is used in transactions.	YES	H	NO	N3	As downloaded from WebTOPs						

FMAXBTH1	MAX BATCH LENGTH The maximum number of transactions allowed before a batch must be settled. It is set to 999.	NO	H	NO	N1-4	As downloaded from WebTOPs
MABA	MERCHANT ABA # Identifies the routing/transit number of the merchant's debit bank, used in transactions. This field is required in Debit transactions.	YES	H	NO	N0-9	As downloaded from WebTOPs
MERNM	MERCHANT NAME Name of the merchant location.	NO	H	NO	X0-20	As downloaded from WebTOPs
MCITY	MERCHANT CITY Identifies the city in which the merchant is located. The first character cannot be a space. This field is used in transactions.	YES	H	NO	X0-11	As downloaded from WebTOPs
MSTAT	MERCHANT STATE Identifies the state in which the merchant resides, used in transactions.	YES	H	NO	X0-2	As downloaded from WebTOPs
MZIP	MERCHANT ZIP CODE Contains the city zip code where the merchant location is. This field is used in transactions.	YES	H	NO	X0-9	As downloaded from WebTOPs
CATCD	MERCH CATEGORY CODE Identifies a merchant industry classification, similar to the SIC (Standard Industry Code). This field is used in transactions.	YES	H	YES	N4	As downloaded from WebTOPs
MLOC	MERCHANT LOCATION # Provides additional information on the location of the merchant, used in transactions.	YES	H	NO	N1-5	As downloaded from WebTOPs
MNUM	MERCHANT NUMBER Unique number that identifies the	YES	H	NO	N0-12	As downloaded from WebTOPs

	merchant to the Exchange system, used in transactions.													
MSETTA	MERCHANT SETTLE AGENT Identifies the merchant’s settling agent for direct debit transactions, used in transactions.	YES	H	NO	N1-4	As downloaded from WebTOPs								
PINBYPASS	PIN BYPASS ALLOWED If enabled then on contact EMV transactions the PIN entry may be skipped by pressing the ENTER key when prompted for the PIN. PIN bypass is NOT allowed on contactless EMV transactions. See Binary Parameter Options in Parameters Overview.	YES	B	NO	B1	As downloaded from WebTOPs								
NFCRDR	NFC READER TYPE Selects the type of NFC Reader supported. <table><tr><th>Display</th><th>Value</th></tr><tr><td>1=NONE</td><td>0</td></tr><tr><td>2=INTERNAL</td><td>5</td></tr><tr><td>3=iPP220</td><td>6</td></tr></table>	Display	Value	1=NONE	0	2=INTERNAL	5	3=iPP220	6	YES	W	YES	N1	As downloaded from WebTOPs
Display	Value													
1=NONE	0													
2=INTERNAL	5													
3=iPP220	6													
QPSPIN	FORCE QPS PIN If QPSPIN is on, the application will prompt for PIN if PIN CVM and equal to or less than QPS limit. This setting can be used if chargebacks are more important than the speed of the transaction.  If QPSPIN is off, the application will not prompt for PIN if PIN CVM and equal to or less than QPS limit. This setting can be used if speed of the	YES	B	NO	B1	As downloaded from WebTOPs								

	transaction is more important than the possible chargebacks.					
TRMID	TERMINAL ID Identifies the POS device's SIP device, used in transactions.	YES	H	YES	N1-8	As downloaded from WebTOPs
TNUM	TERMINAL NUMBER Identifies a unique SIP device within a merchant location, used in transactions.	YES	H	NO	N1-4	As downloaded from WebTOPs
TMDIF	TIME ZONE DIFF Used to calculate the local time within the Exchange host. The differential provides the standard local time zone differential from Greenwich Mean Time (GMT).	YES	W	NO	N3	As downloaded from WebTOPs
AXVOICE	AMEX VOICE AUTH # Phone number used to contact the American Express Authorization Center.	NO	H	NO	X0-14	As downloaded from WebTOPs
DVVOICE	DISCOVER VOICE AUTH # Phone number used to contact the Discover Voice Authorization Center.	NO	H	NO	X0-14	As downloaded from WebTOPs
SVVOICE	SV VOICE AUTH # Phone number used to contact the Stored Value Voice Authorization Center.	NO	H	NO	X0-14	As downloaded from WebTOPs
VMVOICE	VI/MC VOICE AUTH # Phone number used to contact the Visa and MasterCard Voice Authorization Center.	NO	H	NO	X0-14	As downloaded from WebTOPs
STNBYDELAY	STANDBY DELAY Period of inactivity after which the device will go into sleep mode/Standby mode	YES	B	YES	N1-4	As downloaded from WebTOPs

REBOOT24HR	<b>24 HOUR REBOOT</b> Determines if the 24 hour reboot feature is enabled or disabled. It is enabled by default.	YES	H	NO	B1	1
TMIN24HR	<b>MIN REBOOT TIME</b> Specifies the earliest time for the 24 hour reboot. TMIN24HR must be set to a minimum of 30 minutes prior to TMAX24HR.	YES	B	YES	N4	0300
TMAX24HR	<b>MAX REBOOT TIME</b> Specifies the latest time for the 24 hour reboot.	YES	B	YES	N4	0400
PINGURL	<b>PING URL</b> Remote url to verify network	YES	N	NO	X128	www.google.com

## 8.6. Network Parameters

This section contains settings related to Local Area Network dynamic or static IP settings.

**NOTE:** If DHCP is used, the other IP settings are not relevant; they will be overwritten by whatever DHCP assigns to the device.

Parm Name	Description	View/ Print?	Edit?	Edit Reboot?	Type	Default						
NETDHCP	<b>IP ADDRESS ASSIGNMENT</b> Determines if IP address is statically or dynamically. <table><tr><th>Display</th><th>Value</th></tr><tr><td>1=STATIC</td><td>0</td></tr><tr><td>2=DHCP</td><td>1</td></tr></table>	Display	Value	1=STATIC	0	2=DHCP	1	YES	N	YES	B1	As downloaded from WebTOPs
Display	Value											
1=STATIC	0											
2=DHCP	1											



	If 0 (STATIC), the static IP settings below are applied.							
NETTERMIP	IP ADDRESS Terminal’s static IP address. This setting is only applicable if NETDHCP is OFF.	YES	B	YES	X0-15	As downloaded from WebTOPs		
NETMASK	SUBNET MASK Terminal’s subnet mask. This setting is only applicable if NETDHCP is OFF.	YES	B	YES	X0-15	As downloaded from WebTOPs		
NETGATEIP	DEFAULT GATEWAY Terminal’s gateway IP address. This setting is only applicable if NETDHCP is OFF.	YES	B	YES	X0-15	As downloaded from WebTOPs		
NETDNS1IP	DNS SERVER 1 Terminal’s primary DNS IP address. This setting is only applicable if NETDHCP is OFF.	YES	B	YES	X0-15	As downloaded from WebTOPs		
NETDNS2IP	DNS SERVER 2 Terminal’s secondary DNS IP address. This setting is only applicable if NETDHCP is OFF.	YES	B	YES	X0-15	As downloaded from WebTOPs		
POSETHPORT	<b>SIP LISTENING PORT</b> SIP Listening port for POS connected through Ethernet.	YES	B	YES	N1-5	12345		
WIFISSID	NETWORK NAME (SSID) The Wi-Fi System ID.	YES	T	YES	X1-32	Edit on Terminal		
WIFISEC	SECURITY PROTOCOL Determines what type of Wi-Fi Security Mode to use. <table><tr><td>Display</td><td>Value</td></tr></table>	Display	Value	YES	T	YES	N1	Edit on Terminal
Display	Value							

	<table><tr><td>1=WPA2-ENT</td><td>1</td></tr><tr><td>2=WPA2-PSK</td><td>2</td></tr></table>	1=WPA2-ENT	1	2=WPA2-PSK	2									
1=WPA2-ENT	1													
2=WPA2-PSK	2													
WIFIKEY	PRE-SHARED KEY Security key used when security type is WPA2-PSK	YES	T	YES	X8-63	Edit on Terminal								
WIFIAPMAC	ACCESS POINT MAC ADDR The MAC Address of the Wi-Fi Access Point to which the terminal is connected. Contains 00:00:00:00:00:00 when Wi-Fi is not connected.	YES	H	NO	X17-17	Not Editable								
WIFIKEYMGMT	KEY MANAGEMENT The key management protocol used for enterprise is WPA-EAP. <table><tr><th>Display</th><th>Value</th></tr><tr><td>1=WPA-EAP</td><td>1</td></tr><tr><td>2=IEEE 802.1X</td><td>2</td></tr></table>	Display	Value	1=WPA-EAP	1	2=IEEE 802.1X	2	YES	T	YES	X3-16	Edit on Terminal		
Display	Value													
1=WPA-EAP	1													
2=IEEE 802.1X	2													
WIFIWPA	EAP METHOD EAP methods permitted: <table><tr><th>Display</th><th>Value</th></tr><tr><td>1=TLS</td><td>1</td></tr><tr><td>2=PEAP</td><td>2</td></tr><tr><td>3=TTLS</td><td>3</td></tr></table>	Display	Value	1=TLS	1	2=PEAP	2	3=TTLS	3	YES	T	YES	X3-4	Edit on Terminal
Display	Value													
1=TLS	1													
2=PEAP	2													
3=TTLS	3													
WIFIIDENTITY	USERNAME Username used when security type is	YES	T	YES	X1-32	Edit on Terminal								

	WPA2-ENT					
WIFIPASSWSD	PASSWORD Password used when security type is WPA2-ENT.	YES	T	YES	X8-32	Edit on Terminal
ROAMTO	ROAMING TIMEOUT Timeout before displaying WIFI CONNECTION LOST error message.	YES	T	YES	N2	10

## 8.7. Password Parameters

This section contains parameters and password settings for specific functions or menus.

The application supports 3 levels of passwords: Administrator, Manager (MPWD), and Supervisor (SPWD).

- All Password Level settings below provide the same options.

Display	Value
1=NONE	0
2=SUPERVISOR	1
3=MANAGER	2
4=ADMIN	3

- The administrator password can be used at a screen protected by manager, supervisor, or admin password. The administrator password is the current day of year x 2. If the admin password is less than 3 digits, leading zeroes must be keyed in to enforce a length of 3. The password changes daily to meet PCI requirements.
- The manager password can be used at a screen protected by manager or supervisor.
- The supervisor password can only be used at supervisor password protected screens.

**NOTE:** Passwords allow entry of up to 12 characters even though in practice, the merchant can only choose a 5-8 character value. This is to prevent attackers from knowing the target number of characters in the real password.

Parm Name	Description	View/	Edit?	Edit	Type	Default
-----------	-------------	-------	-------	------	------	---------

		Pri nt?		Re bo ot?		
SPWD	SUPERVISOR PASSWORD Password used to gain access to a supervisor function.	NO	W	NO	X5-8	As downloaded from WebTOPs
MPWD	MANAGER PASSWORD Password used to gain access to a manager, or supervisor function.	NO	W	NO	X5-8	As downloaded from WebTOPs

## 8.8. Transaction Parameters

This section contains parameters specific to transaction processing.

Parm Name	Description	Vie w/ Pri nt?	Edi t?	Edit Reb oot ?	Type	Default
BATNUM	BATCH NUMBER The batch number can be changed to renumber the batch or begin numbering the batches starting with a specific number. This field is used in transaction processing and needs values of 001 to 999. * Use the Batch Change function to edit the batch number.	YES	T*	NO	N3	1
CASHBACK	DEBIT CASHBACK SUPPORT Specifies if cashback prompts and other cashback related processing is enabled for PIN Debit transactions.	YES	B	NO	B1	As downloaded from WebTOPs
EBTCASHBACK	EBT CASHBACK SUPPORT Specifies if cashback prompts and other cashback related processing is enabled for EBT Cash Benefits transactions.	YES	B	NO	B1	As downloaded from WebTOPs

CBLIMIT	CASHBACK LIMIT Specified the maximum allowable cashback amount (in cents). Must be set in the range of \$50.00 to \$200.00.	YES	W	NO	N4-5	As downloaded from WebTOPs
CBASSIST	CASHBACK ASSIST Specifies if cashback assist prompting is enabled.	YES	B	NO	B1	As downloaded from WebTOPs
CBAST1	CASHBACK ASSIST AMOUNT 1 Specifies the first suggested cashback amount (in whole dollars) to be displayed on the cashback assist prompt.	YES	B	NO	N2-3	As downloaded from WebTOPs
CBAST2	CASHBACK ASSIST AMOUNT 2 Specifies the second suggested cashback amount (in whole dollars) to be displayed on the cashback assist prompt.	YES	B	NO	N2-3	As downloaded from WebTOPs
CBAST3	CASHBACK ASSIST AMOUNT 3 Specifies the third suggested cashback amount (in whole dollars) to be displayed on the cashback assist prompt.	YES	B	NO	N2-3	As downloaded from WebTOPs
EMV	EMV ENABLED If enabled then allows the merchant to process EMV transactions.	YES	B	YES	B1	As downloaded from WebTOPs
EMVNEW	EMV PDL AVAILABLE This flag is set to indicate that the terminal needs to perform an EMV PDL.	YES	B	YES	B1	As downloaded from WebTOPs
EMVBEEP	EMV BEEP ENABLED If enabled then the SIP device will beep every 3 seconds when prompting the operator to remove an EMV card.	YES	B	NO	B1	As downloaded from WebTOPs

EMVCONV	TRAN REF CURRENCY CNV Transaction Reference Currency Exponent – Factor used in the conversion from the Transaction Currency Code to the Transaction Reference Currency Code.	NO	H	NO	N8	As downloaded from WebTOPs								
PDLDIAG	PDL DIAGNOSTICS This enables EMV diagnostics for troubleshooting.	YES	B	NO	B1	As downloaded from WebTOPs								
GIFT	GIFT ALLOWED Determines if Gift card transactions are supported. See Binary Parameter Options in Parameters Overview.	YES	W	NO	B1	As downloaded from WebTOPs								
MANUAL	MANUAL ENTRY Specifies if manual entry is allowed.	NO	B	YES	B1	As downloaded from WebTOPs								
STORMD	SAF MODE *The Set Store and Forward function is used to set this value. <table><tr><th>Display</th><th>Value</th></tr><tr><td>1=OFF</td><td>0</td></tr><tr><td>2=ALWAYS</td><td>1</td></tr><tr><td>4=AUTO</td><td>3</td></tr></table> In SIP mode acceptable values are (0, 1 and 3). The value 2 is applicable for stand-alone mode.	Display	Value	1=OFF	0	2=ALWAYS	1	4=AUTO	3	YES	B*	NO	N1	As downloaded from WebTOPs
Display	Value													
1=OFF	0													
2=ALWAYS	1													
4=AUTO	3													
STORFL	SAF AMOUNT MAX Maximum amount (in pennies) that can be used for a Store and Forward	NO	W	NO	N1-6	As downloaded from								

	transaction.					WebTOPs								
STORLMT	SAF PENDING LIMIT Maximum number of pending unauthorized transactions that can be stored in a batch.	NO	W	NO	N1-3	As downloaded from WebTOPs								
STLVOIDS	SETTLE ALLOW VOIDS Enables/disables voids after settlement. See Binary Parameter Options in Parameters Overview.	YES	T	NO	B1	1								
TIP	TIP SUPPORT Enables/disables prompting for tip. <table><tr><th>Display</th><th>Value</th></tr><tr><td>1=OFF</td><td>0</td></tr><tr><td>2=PROMPT</td><td>1</td></tr><tr><td>3=PRINT</td><td>2</td></tr></table>	Display	Value	1=OFF	0	2=PROMPT	1	3=PRINT	2	YES	B	NO	N1	As downloaded from WebTOPs
Display	Value													
1=OFF	0													
2=PROMPT	1													
3=PRINT	2													
TIPAST1	TIP ASSISTANCE 1 This is the first suggested tip percentage displayed in the tip assist logic. The default value is 1000 which is 10% of the total sale amount. It does not support fractional value like 1025 (10.25%) due to display size limitation.	YES	B	NO	N1-4	1000								
TIPAST2	TIP ASSISTANCE 2 This is the second suggested tip percentage displayed in the tip assist logic. The default value is 1500 which is 15% of the total sale amount. It does not support fractional value like 1550 (15.50%) due to display size limitation.	YES	B	NO	N1-4	1500								
TIPAST3	TIP ASSISTANCE 3 This is the third suggested tip percentage displayed in the tip assist	YES	B	NO	N1-4	2000								

	logic. The default value is 2000 which is 20% of the total sale amount. It does not support fractional value like 2075 (20.75%) due to display size limitation.											
WANTTOTIP	<div>WANT TO TIP PROMPT Enables/disables prompting as to whether the cardholder wants to enter a tip if POS sends Sale request without tip amount included (&lt;TipAmount&gt;).</div> <table><tr><th>Display</th><th>Value</th></tr><tr><td>1=OFF</td><td>0</td></tr><tr><td>2=PROMPT</td><td>1</td></tr></table>	Display	Value	1=OFF	0	2=PROMPT	1	YES	B	NO	B1	As downloaded from WebTOPs
Display	Value											
1=OFF	0											
2=PROMPT	1											
WHITELIST	<div>WHITELIST Used to enable whitelisting functionality to return whitelisted, non-bank cards to POS.</div>	YES	W	NO	B1	As downloaded from WebTOPs						
EODAUTO	<div>AUTO EOD PROC Enables/disables auto EOD processing occurring at EODTIMER value.</div>	YES	B	YES	B1	As downloaded from WebTOPs						
EODTIMER	<div>EOD PROC TIME Time of the day at which EOD processing will begin automatically.</div>	YES	B	YES	N0-6	As downloaded from WebTOPs						
BATCHCLOSE	<div>BATCH CLOSE Enables/disables batch close as a part of EOD processing.</div>	YES	B	NO	B1	As downloaded from WebTOPs						
POSNOTIFY	<div>POS NOTIFICATION MESSAGES Enables/disables POS notification messages.</div>	YES	B	NO	B1	As downloaded from WebTOPs						
QCHIP	<div>QUICK CHIP</div>	NO	H	NO	B1	As						



	Enables/disables Quick Chip processing. NOTE: Quick Chip is always enabled for U.S. deployments.					downloaded from WebTOPs								
QCHIPAMT	QUICK CHIP AMOUNT Amount (in cents) to be used as the Quick Chip predetermined amount when the StartCard command is used.	YES	W	NO	N1-6	As downloaded from WebTOPs								
CANCELKEY	CANCEL KEY Configures the cancel key behavior. <table><tr><th>Display</th><th>Value</th></tr><tr><td>CANCEL</td><td>1</td></tr><tr><td>SKIP</td><td>2</td></tr><tr><td>IGNORE</td><td>3</td></tr></table> Refer to <a href="#">Cancel Key Configuration</a> section for more details.	Display	Value	CANCEL	1	SKIP	2	IGNORE	3	YES	W	NO	N1	1
Display	Value													
CANCEL	1													
SKIP	2													
IGNORE	3													
CRDCATPRMPT	CARD CATEGORY PROMPT Configure the card category prompting options. <table><tr><th>Display</th><th>Value</th></tr><tr><td>DISABLED</td><td>0</td></tr><tr><td>ENABLED</td><td>1</td></tr><tr><td>CONDITIONAL</td><td>2</td></tr></table> Refer to <a href="#">Card Type Determination</a> section for more details.	Display	Value	DISABLED	0	ENABLED	1	CONDITIONAL	2	YES	W	NO	N1	1
Display	Value													
DISABLED	0													
ENABLED	1													
CONDITIONAL	2													
BATCHRPTEOD	BATCH REPORT ON EOD Enabling/Disabling the inclusion of batch summary and details in EOD reports/receipt	YES	B	NO	B1	1								

REMOVECARDWAIT	<p><b>REMOVE CARD WAIT</b></p> <p>Determines when the final REMOVE CARD prompt occurs. This prompt blocks further processing until the user removes their card.</p> <ul style="list-style-type: none"><li>● AFTER EMV: Before host communications when EMV card processing is finished.</li><li>-or-</li><li>● AFTER POS RESET: After host communications when the POS sends the Reset command to conclude the transaction.</li></ul> <p><b>Note:</b> Parameter is used in Sale, StartCard, Refund and CreditAuth commands only.</p> <table><tr><th>Display</th><th>Value</th></tr><tr><td>AFTER EMV</td><td>1</td></tr><tr><td>AFTER POS RESET</td><td>2</td></tr></table>	Display	Value	AFTER EMV	1	AFTER POS RESET	2	YES	B	NO	N1	2
Display	Value											
AFTER EMV	1											
AFTER POS RESET	2											
EMVDRLn where n = 1-16	<p><b>DYNAMIC READER LIMIT n</b></p> <p>This is the n-th set of Dynamic Reader Limits (DRL). Each set of DRL has the following fields separated by “.”:</p> <ul style="list-style-type: none"><li>● <u>Set ID</u> in HEX format with up to 2 digits length.</li><li>● <u>Contactless Transaction Limit</u> in BCD format with up to 12 digits.</li><li>● <u>CVM Required Limit</u> in BCD format with up to 12 digits.</li><li>● <u>Contactless Floor Limit</u> in BCD format with up to 12 digits.</li></ul>	NO	W	NO	X0-41	As downloaded from WebTOPs						

## 8.9. Serial Parameters

This section contains parameters specific to serial communications with the POS.

Parm Name	Description	View/Print?	Edit?	Edit Reboot?	Type	Default	
COMMSIPPORT	SIP<->POS LINK TYPE Used when POSLNKTYP set to serial to define the serial port used for POS to SIP communications.	NO	B	NO	N1	3	
	Display						Value
	RS-232 RJ-12						1
	USB						2
	RS-232 DB-9						3
COMMBAUD	BAUD RATE Baud rate used for serial communications between the POS and SIP device.	NO	B	No	N1	6	
	Display						Value
	1200						1
	2400						2
	9600						3
	19200						4
	38400						5
	115200						6
COMMFORMAT	FORMAT Specifies format used for serial communications between POS and SIP device, first digit is word	NO	B	NO	N1	5	

size, 2<sup>nd</sup> character is parity (Even, Odd, None),  
third is number of stop bits.

Display	Value
7E1	1
7N1	2
7O1	3
8E1	4
8N1	5
8O1	6

## 8.10. Credential Sharing Between Downloader and HPA

The Heartloader and HPA applications share the same WiFi credentials which are stored in the COMMLINK.CFG file located in the Host folder and available to both applications.

If the terminal is not a Wi-Fi capable terminal, then the COMMLINK.CFG file contains KEY=VALUE pairs of the fields shown below.

Field	Value	Description
SIP Listening Port	1-5N	SIP Listening port for POS connected through IP.
POS Connection	1N	This parameter decides which interface is used for IP communication. 1: SERIAL 2: ETHERNET 3: WIFI
Serial Protocol	1N	Used to define the serial port used for POS to SIP communications. 1: RS-232 RJ-12 2: USB 3: RS-232 DB-9

Baud Rate	1N	Baud rate used for serial communications between the POS and SIP device. 1: 1200 2: 2400 3: 4800 4: 9600 5: 14400 6: 19200 7: 38400 8: 57600 9: 115200
Data Format	1N	Specifies the format used for serial communications between POS and SIP device: 1st digit is the word size, 2nd character is the parity (Even, Odd, None), and 3rd digit is the number of stop bits. 1: 7E1 2: 7N1 3: 7O1 4: 8E1 5: 8N1 6: 8O1 7: 7N2
IP Address Assignment	1N	0: Static 1: DHCP
IP Address	7-128N	IP address of the terminal
Default Gateway	7-128N	IP address of the gateway
Subnet Mask	1-128N	Subnet mask
DNS Server 1	7-128N	IP address of DNS server 1
DNS Server 2	0-128N	IP address of DNS server 2

If the terminal is a Wi-Fi capable terminal, in addition to the fields in the table above the file contains the fields shown below.

Field	Value	Description
Wi-Fi Security	1N	The type of Wi-Fi security being used. 1 = WPA2-Enterprise 3 = WPA2-Personal
Wi-Fi SSID	1-32X	Wi-Fi SSID
Wi-Fi Key	8-63X	Security key used when security type is WPA2-PSK
Wi-Fi Key Management	3-16X	Decides why key type to use when security type is WPA2-Enterprise
Wi-Fi EAP Method	3-4X	The EAP methods permitted include PEAP, TTLS, and TLS
Wi-Fi Login	8-32X	Username used when security type is WPA2-ENT
Wi-Fi Password	1-32X	Password used when security type is WPA2-ENT

A fresh terminal is loaded with the terminal baseline and the Heartloader application. The Heartloader application is used to download the HPA application from the Heartland Universal Download System (HUDS).

Since Heartloader is used to download HPA, the WiFi credentials are established using the Heartloader application. The Heartloader application stores the WiFi credentials on the terminal in a COMMLINK.CFG file stored in the Host folder.

HPA reads the WiFi credentials from the COMMLINK.CFG file and uses those to establish the WiFi connection.

HPA provides the ability to change the WiFi credentials should the need arise.

## 9. Appendices

### 9.1. Glossary

- AAC: Application Authentication Cryptogram, a type of application cryptogram generated by the chip housed in an EMV card when a card declines a transaction during Card Action Analysis
- AC: Application Cryptogram, generated by the chip housed in an EMV card
- App ID: Application ID number, a unique alphanumeric reference to a payment or supporting application that is downloaded from HUDS

- ARQC: Authorization Request Cryptogram, generated by the card issuer on an EMV transaction
- AVS: Address Verification System, used to verify the address of the person claiming to own the card
- CVM: Cardholder Verification Method, the CVM is provided by an EMV card and defines any supported or preferred methods for a cardholder to verify a transaction. Additional factors may determine which CVMs are supported on a given TID
- CVV: Card Verification Value, a verification code printed on the back of the card
- DHCP: Dynamic Host Configuration Protocol, an automatic client/server protocol
- DUKPT: Derived Unique Key Per Transaction, a key management scheme in which for every transaction, a unique key is used which is derived from a fixed key
- ECR: Electronic Cash Register
- EMV: Europay, Mastercard, Visa
- EMV PDL: EMV Parameter Download, this refers specifically to EMV parameters defined by card brands
- EOD: End of Day, a process which resolves any pending transactions held locally in a terminal or SIP device
- Exchange: The Heartland front-end authorization system which routes authorization requests to issuers
- HPS: Heartland Payment Systems
- HSC: Heartland Service Center
- HUDS: Heartland Universal Download System, provides application and parameter files to terminals
- Infocentral: Heartland System which provides merchant reporting on transaction activity
- LLT: Local Loading Tool, provides download/upload access to the device
- PCI scope: Payment Card Industry scope, environment which accepts and processes credit card payments
- PDL: Parameter Download, this may be used in reference to either application parameters or EMV parameters defined by card brands (EMV PDL)
- POS: Point of Sale

- QPS: Quick Payment Service, used here as a catch-all term which allows foregoing certain CVM methods based on individual factors of a transaction, e.g. authorization amount
- RID: Registered Application Identifier numbering system provides a means for an application and related services offered by a provider to identify if a given card contains the elements required by its application and related services.
- SAF: Store And Forward, allows for card processing during periods of outage or maintenance of core systems.
- SDK: Software Development Kit, provided to facilitate specific platform interaction.
- SIP: Semi-Integrated Peripheral
- SIP Device: Any terminal or PIN pad which runs the payment engine and interfaces with a POS or ECR
- TID: Terminal ID number, a unique alphanumeric reference to application and parameter files managed in HUDS
- TMS: Terminal Management System, any system which manages terminal application or parameter files. For HPA, the TMS is HUDS
- WebTOPs: A browser-based system used by Heartland to create and update TIDs
- XML: Extensible Markup Language, defined message text; used for HPA communications

## 9.2. BIN Table

### 9.2.1. Overview

The following section outlines the BIN table format. The BIN table is comprised of parameters that are downloaded as names BIN01-BIN99.

Each field in a row is delimited by a period. All fields are variable length; the Length column indicates the maximum supported length.

All properties for a given card type except for the PAN ranges and min/max lengths are assumed to be the same. They should not be set different for testing for a given card type. The application will consider the values of the first entry for a given card type and use these values for the rest of the entries of the same card type. This is because in practice, WebTOPs (used to manage parameters) will only allow changing settings for an entire card type.

Development and testing should take this into consideration when designing application features.



Field	Len	Description
RangeEnabled	1	Indicates if card range is enabled: 0=Off, 1=On
PanLow	10	Beginning BIN range
PanHigh	10	Ending BIN range
ShortName	3	2-3 character short name for the card type
CardName	16	Long name of card type
MinLength	2	Minimum PAN length for card
MaxLength	2	Maximum PAN length for card. This value may be set up to 19 digits.
SecurityCode	1	Card security code prompt enabled: 0=Off, 1=On, 2=Card not present
AllowTip	1	Tip support: 0=Off, 1=Prompt on purchase, 2=Tip supported but don't prompt on purchase Tips can be edited on credit cards if this setting is 1 or 2 for the card type. NO LONGER USED.
TipDiscount	3	Tip discount percentage. 3 digits are applied like this: x.xx%
QPSLimit	6	QPS limit in pennies
ExpDate	1	Expiration date check enabled: 0=Off, 1=On; This flag is ignored and the Expiration Date not validated if the CardType is EBT. If the flag is disabled, an Expiration Date of 12/49 (MM/YY) will be used.
ManualEntry	1	This field is currently unused
AVS	1	Address Verification Service supported for card: 0=Off, 1=On

Cashback	1	Cashback prompted for card: 0=Off, 1=On. NO LONGER USED.
CardType	1	Card type: 1 = Visa, 2= MasterCard, 3=American Express, 4=Discover, 5=Other credit card, 6=Debit, 7=EBT, 8=HPS Stored Value, 9=HPS Gift/Rewards, 11=PayPal  Note: If "Other" credit card is used, the same label should be used for all BIN ranges of type 5, such as "Misc card". This label is used on receipts and reports and all totals for this card type are grouped as one.
LuhnCheck	1	Luhn check the card: 0=Off, 1=On

### 9.2.2. Sample BIN Table

**DISCLAIMER:** This sample BIN table is only a sample to help define the actual BIN table values. The actual values would get downloaded from WebTOPs. The actual values cannot be shown here as they change from time to time.

Not all options are applicable to all functions/card types. For example, manual entry on debit transactions is not allowed even if the flag in the table is enabled. Individual transaction flows describe all available options for the card type/function.

B I N #	PAN Low	PAN High	S h o r t  N a m e	Card Name	M i n  L e n	M a x  L e n	S e c u r i t y  C o d e	A l l o w  T i p	Tip Dis c	QPS Limit	E x p  D a t e  C h e c k	M a n u a l  E n t r y	A V S	C a s h b a c k	C a r d  T y p e	L u h n  C h e c k
1	4000000000	4999999999	VI	Visa	13	19	2	0	000	0000	1	1	0	0	1	1
2	2221000000	2720999999	MC	Mastercard	16	19	1	0	000	0000	1	1	0	0	2	1
3	5100000000	5599999999	MC	Mastercard	16	19	1	0	000	0000	1	1	0	0	2	1
4	3400000000	3499999999	AX	American Express	15	15	1	0	000	0000	1	1	0	0	3	1

5	3700000000	3799999999	AX	American Express	15	15	1	0	000	0000	1	1	0	0	3	1
6	3000000000	3059999999	DV	Discover	16	19	1	0	000	0000	1	1	0	0	4	1
7	3095000000	3095999999	DV	Discover	16	19	1	0	000	0000	1	1	0	0	4	1
8	3528000000	3589999999	DV	Discover	16	19	1	0	000	0000	1	1	0	0	4	1
9	3600000000	3699999999	DV	Discover	14	19	1	0	000	0000	1	1	0	0	4	1
10	3800000000	3999999999	DV	Discover	16	19	1	0	000	0000	1	1	0	0	4	1
11	6011000000	6011039999	DV	Discover	16	19	1	0	000	0000	1	1	0	0	4	1
12	3088000000	3094999999	DV	JCB	16	19	1	0	000	0000	1	1	0	0	4	1
13	3096000000	3102999999	DV	JCB	16	19	1	0	000	0000	1	1	0	0	4	1
14	3112000000	3120999999	DV	JCB	16	19	1	0	000	0000	1	1	0	0	4	1
15	3158000000	3159999999	DV	JCB	16	19	1	0	000	0000	1	1	0	0	4	1
16	3337000000	3349999999	DV	JCB	16	19	1	0	000	0000	1	1	0	0	4	1
17	6011040000	6011049999	PP	PayPal	16	19	0	0	000	0000	1	1	0	0	11	1
18	6011050000	6011099999	DV	Discover	16	19	1	0	000	0000	1	1	0	0	4	1
19	6011200000	6011999999	DV	Discover	16	19	1	0	000	0000	1	1	0	0	4	1
20	6221260000	6229259999	DV	Discover	16	19	1	0	000	0000	1	1	0	0	4	1
21	6240000000	6269999999	DV	Discover	16	19	1	0	000	0000	1	1	0	0	4	1
22	6282000000	6288999999	DV	Discover	16	19	1	0	000	0000	1	1	0	0	4	1
23	6440000000	6505999999	DV	Discover	16	19	1	0	000	0000	1	1	0	0	4	1
24	8100000000	8109999999	DV	UnionPay	16	19	1	0	000	000	1	1	0	0	4	1
25	8110000000	8131999999	DV	UnionPay	16	19	1	0	000	000	1	1	0	0	4	1

26	8132000000	8151999999	DV	UnionPay	16	19	1	0	000	000	1	1	0	0	4	1
27	8152000000	8163999999	DV	UnionPay	16	19	1	0	000	000	1	1	0	0	4	1
28	8164000000	8171999999	DV	UnionPay	16	19	1	0	000	000	1	1	0	0	4	1
29	6506000000	6506009999	PP	PayPal	16	19	0	0	000	0000	1	1	0	0	11	1
30	6506010000	6506099999	DV	Discover	16	19	1	0	000	0000	1	1	0	0	4	1
31	6506100000	6506109999	PP	PayPal	16	19	0	0	000	0000	1	1	0	0	11	1
32	6506110000	6599999999	DV	Discover	16	19	0	0	000	0000	1	1	0	0	4	1
33	5878540000	5878549999	SV	Stored Value	16	16	0	0	000	0000	0	1	0	0	8	1
34	6018130000	6018139999	SV	Stored Value	16	16	0	0	000	0000	0	1	0	0	8	1
35	6050370000	6050379999	SV	Stored Value	16	16	0	0	000	0000	0	1	0	0	8	1
36	6064340000	6064349999	SV	Stored Value	16	16	0	0	000	0000	0	1	0	0	8	1
37	6274071000	6274071009	SV	Stored Value	16	16	0	0	000	0000	0	1	0	0	8	1
38	6277220000	6277229999	SV	Stored Value	16	16	0	0	000	0000	0	1	0	0	8	1
39	6299290000	6299299999	SV	Stored Value	16	16	0	0	000	0000	0	1	0	0	8	1
40	5022440000	5022449999	HG	Heartland Gift	19	19	0	0	000	0000	0	1	0	0	9	1
41	6277200000	6277209999	HG	Heartland Gift	16	16	0	0	000	0000	0	1	0	0	9	1
42	0000000000	9999999999	DBT	Debit	13	19	0	0	000	0000	0	0	0	0	6	0
43	0000000000	9999999999	EBT	EBT	13	19	0	0	000	0000	0	1	0	0	7	0
44	0000000000	9999999999	HG	Heartland Gift	5	19	0	0	000	0000	0	1	0	0	9	0

### 9.2.3. BIN Range Setup

- The application can maintain a maximum of 99 BIN ranges. These BIN ranges can be set using parameters BIN01 to BIN99. These values are stored in the terminal application and will persist across a power failure.
- The application will process downloaded parameter values only when BINNEW parameter is equal to 1. This is to prevent accidental update of the BIN range parameter values.
- A BIN range can be deleted by downloading the parameter with value set to "0". For example, downloading BIN01="0" will remove the BIN01 range from BIN ranges used for card processing.

Once removed, a BIN range can be added back by setting the parameter using valid values as described above.

- The all-inclusive ranges (0000000000 – 9999999999) need to be placed to the bottom of the BIN range list so that cards swiped at idle can be identified. See Idle Screen Overview for more details.
- The all-inclusive HGM range needs to be placed after Debit to avoid initiating a Gift Redeem when a card is swiped at idle that does not fall in any of the defined BIN ranges (for example a Debit or EBT card).

#### 9.2.4. BIN Range Validation

- The application validates the card account number against a set of BIN ranges to prevent the user using unwanted cards. This validation process is explained in detail below.
- During a transaction, the card type or category is identified by the menu selected. When a card is swiped or manually entered, the card account number is validated against this set of BIN ranges.
- When Track1 and Track2 data is not available then the terminal would display error message "BAD CARD READ". If Track1 data is available, but Track2 data is not available and Track2 data required, Terminal will display error message "PARTIAL CARD READ".

If a BIN range is found that is enabled, matches the card type and min and max lengths, the card is accepted. If not, the card is rejected and the Application Error screen executes with "CARD NOT SUPPORTED" if the BIN range is not found, else with "CARD NOT ALLOWED" if the card type does not match, else with "BAD CARD LENGTH" if the length falls outside of min and max. After pressing a key the clerk will be returned to the previous prompt so they can enter a valid value.

#### 9.2.5. Security Code

The card security code (a.k.a. CAV2/CID/CVC2/CVV2), when enabled, is used for fraud protection on manually entered transactions. Prompt only if the card number was manually entered and the SecurityCode parameter is enabled in the BIN table for the associated card type.

- Card Verification is supported on MasterCard, American Express, and Discover cards only.
- MasterCard and Discover cards use a three-digit code. American Express uses a four-digit code.

#### 9.2.6. Tip Discount Rate

- Tip discounting, when enabled, allows the merchant to compute the fee amount the clerk/server should pay for tips on credit card sales. This feature is often used in the restaurant

industry but can be used in the retail industry. The Tip Discount rate only impacts the Tip Discount and IRS Tip reports. The format of this field is 9v99 (e.g. 150 = 5.50%).

### 9.2.7. B.7 QPS Limit

- QPS Limit sets a floor amount for Quick Payment Service transactions (credit sale, only). The floor amount includes the base amount + tip + tax applied to the sale.
- QPS Limit does not apply to credit sale where the card acquisition was done manually.
- The QPSQualified flag returned to the POS for credit sale transactions allows the transactions under or equal to the QPS Limit amount to print QPS credit sale receipts using QPS rules and settings when set or the normal credit sale receipts when not set.
- Normally, tips are turned off in the parameters for a QPS merchant. But technically, it can be turned on in the application. If tip is on, the total amount (amount + tip) is compared with the QPS Limit. Tips can also be adjusted.
- The QPS limit for contactless will be set in the RID file for the card brand in the CVM Required Limit
- When the credit sale is under the QPS limit the EMV contact and contactless card transactions will not require any cardholder verification method, meaning signature or PIN entry for non-SAF transactions (unless otherwise configured).

### 9.2.8. Expiration Date Check

- If Expiration Check is enabled for a BIN range, the application checks the expiration date of the card. If a card is swiped, the expiration date is obtained from the card track data. If a card is manually entered, the expiration date is prompted.
- If the expiration date is incorrect (invalid month), the Application Error screen executes with "INCORRECT DATE". If the card is expired, the Application Error screen executes with "CARD EXPIRED". After pressing a key the clerk will be returned to the previous prompt.
- Typically, only Visa, MasterCard, American Express, and Discover cards are checked for valid expiration dates. PIN based debit, EBT, GSB/Stored Value, and HMS Gift/Rewards cards are usually not checked for expiration dates or expired entered expiration dates. However, the application supports configuring these card types for expiration dates in case this policy changes in the future.

### 9.2.9. AVS

- Address Verification Service (AVS) is used for fraud protection on manually entered credit card transactions. An overview of AVS follows:
  - AVS is only prompted for on Visa, MasterCard, American Express, and Discover credit cards.
  - The Street Address Number allows up to 19 digits to be entered.
  - The ZIP Code is either five or nine digits in length.
- An AVS mismatch occurs when the host sends an AVS response that is A, N, or Z (if street address sent). Note that the Z response indicates that only the zip code matched, so this response is not considered a mismatch if only the zip code was sent.
- When a mismatch occurs, the user has the option to proceed or cancel the transaction. A reversal is automatically sent on credit card transactions if the terminal times out or the user chooses cancellation.

### 9.2.10. Manual Entry Allowed

This field is unused in this application and only exists for compatibility with prior application WebTOPs management. Manual Entry support is determined by the transaction type.

### 9.2.11. Luhn Check

- If Luhn check is enabled for a BIN range, the application performs standard Luhn (Mod-10) check on the account number.
- For E3 transactions, the Luhn check status is provided by the E3 card API; it cannot be calculated by software.
- If Luhn check fails on the account number, the Application Error screen executes with “BAD ACCOUNT #”. After pressing a key the clerk will be returned to the previous prompt so they can enter a valid value.

## 9.3. EMV PDL Setup

EMV PDL system uses the following parameters to identify the EMV PDL parameters sent in a PDL download response:

- MID (Merchant ID)
- TNUM (Terminal or Lane Number)

These need to be setup in the EMV PDL database by sending a request to POS Integrations.

## 9.4. Portico Setup

Portico authenticates transactions using:

- Site ID (maps to MID)
- License ID
- Device ID (maps to TNUM)
- Username
- Password

These need to be setup in Portico database by sending a request to POS Integrations.

Portico in turn uses its internal MID & TNUM to communicate with Exchange.

## 9.5. HUDS Setup

HUDS uses the following parameters to identify the software package to be downloaded:

- APPID (Application ID)
- TID (Terminal ID)

These need to be setup in the HUDS database by sending a request to POS Integrations.

The MID and TNUM are parameters for a specific TID.

## 9.6. HPA SDK

### 9.6.1. Overview

The HPA SDK consists of four components:

- HeartLoader application – This application is included in the terminal baseline (the files making up the terminal operating system) and is used to load the HPA application from the Heartland Universal Download System (HUDS).
- HeartClean application – This application is also included in the terminal baseline and is used to remove pre-existing applications from the terminal. The associated HSIPCOMPS.TXT file contains the list of components that HeartClean will not remove from the system. HeartClean only executes once when the baseline is installed. After running the first time, HeartClean will delete itself.



- HPA application – This is the application that executes on the SIP device (for example, the Lane/5000). This application processes transaction requests received from the POS, acquires the payment card and authorizes the transaction with the Host.
- HeartPOS application – This is a stand-alone Windows application to provide an example Point Of Sale system to demonstrate processing transactions with HPA. This SDK also contains the source code for the HeartPOS application, which has been written in C# and requires Microsoft Visual Studio 2013 to compile and execute.

## 9.7. HPA Installation

### 9.7.1. Installation Overview

If the terminal has the current baseline installed then HPA may be downloaded using the HeartLoader application as described in section 10.7. Terminals shipped from Ingenico or from the Heartland Service Center should have the terminal baseline with HeartLoader installed.

If the terminal is running RBA or if the terminal does not have the current version of the baseline installed then the following process should be used:

- Set the terminal date and time
- Clean the terminal.
- Install the terminal baseline which includes the HeartLoader application.
- Inject test keys (development terminals only, production terminals should already have keys injected.)
- Use the HeartLoader application to download the HPA application from the Heartland Universal Download System (HUDS).

### 9.7.2. Set the terminal date and time

To install HPA it is important that the device's system date and time be set to the current date and time. Terminals with factory settings may have a system date that is not current. Terminals with pre-loaded applications will have the system date set correctly and the next step may be skipped.

To set system date on a terminal, let the factory installed default application boot up completely. Please press F key (or + key if device is iSC), then select Telium Manager, then Initialization, then Parameters, then Date & Time. Set the date and time.

### 9.7.3. Clean the Terminal

If the terminal is not running RBA then it is cleaned by clearing the terminal memory. The process for clearing the terminal memory is:

- Reboot the device. To reboot, press and hold the CLEAR and the “.,#\*” keys simultaneously.
- When the "Welcome" screen with colored dots is shown, press and hold the "-.,#\*” key immediately.
- The terminal should now display a picture of a folder with a green arrow pointing down.
- You may have to do the above steps a couple of times to get the timing correct. If the picture of the folder is not displayed on the screen, then re-boot the terminal and repeat the above steps.
- Open LLT and connect it to the device.
- In the upper left corner of LLT, click on the “Show the installed components” button - box icon. Then click the broom icon “Clean the terminal”. LLT will now prompt for confirmation if we are sure to remove all components on the terminal. Click okay and disconnect LLT.
- Terminal will now reboot and it should come back to the picture of a folder with a green arrow pointing down.

If the terminal is running RBA then instead of clearing the memory please follow the process described below in section [Field Upgrade by Merchants Running RBA](#).

### 9.7.4. Baseline Installation Overview

The terminal baseline with HeartLoader can be installed in a few ways:

- Install using the Ingenico LLT application
- Installed using a batch file included in the SDK (this also requires Ingenico LLT application be installed)
- RBA Field Upgrade for terminals that have the RBA application installed.

### 9.7.5. Installing Baseline/HeartLoader Using LLT

#### 9.7.5.1. Baseline with HeartLoader Installation on Lane/3000 and Lane/5000

- Install the LLT tool .
- Connect terminal to PC using USB Serial cable.
- Clear the terminal memory as described in section [Clean the Terminal](#).

- **IMPORTANT:** Note that after clearing memory it is critical to reboot the terminal for the terminal to restore the HOST folder. Verify that the HOST folder is present on the terminal using LLT prior to running HeartLoader.bat. Failure to reboot the terminal after clearing memory will result in rendering the terminal inoperable.
- Configure LLT and connect it to the device.
- Download ..\HPA\Ingenico\Lane3000\HeartLoaderPackage\Installer\HLOADER.M83 for Lane/3000.
- Download ..\HPA\Ingenico\Lane5000\HeartLoaderPackage\Installer\HLOADER.M72 for Lane/5000.
- Disconnect LLT and the device will reboot.
- After loading the baseline and HeartLoader, development terminals will go to the key injection state (production terminals should already have production keys injected). The test keys should then be loaded as described in section [Loading Test DUKPT/EMV keys](#).

## 9.7.6. Field Upgrade By Merchants Running RBA

### 9.7.6.1. Prerequisites

- Make sure the terminal is using the US Common Profile ( see section 10.11). Typically, RBA is signed with the US Common Profile by Ingenico and HeartLoader is signed by US Common Profile by Heartland. You can only upgrade from one app to the other if they are both signed by the same profile. For example, you cannot upgrade or install from the Mock profile to the US Common Profile.
- Make sure the terminal has the HPS Production DUKPT keys, which are also used for EMV PIN.
- If the terminal is not on US Common Profile or if it does not have HPS Production DUKPT keys, it needs to be shipped to the Heartland Service Center to have the keys loaded in a secure facility. You may need a swap of your terminal.
- Heartland does not support RKI (Remote Key Injection).

### 9.7.6.2. Point Of Sale Development for Upgrading RBA Terminals

- Connect the SIP device running RBA to your POS system.
- Make sure RBA is running.
- Clear any previous transactions from the SIP device. You may have to close your existing batch.

- Code your POS application to use the RBA “File Write” command to send the OGZ file to the terminal.
- For the Lane/5000 terminal the OGZ file is  
..\HPA\Ingenico\Lane5000\HeartLoaderPackage\Installer\HLPackage.OGZ.
- Code your POS application to reboot the SIP device.
- Refer to Ingenico’s RBA guide for details on the File Write and Reboot commands.
- The SIP device will go through a few reboots and upgrade itself to the HeartLoader app without user intervention.

### 9.7.7. Loading Test DUKPT/EMV keys

#### 9.7.7.1. Overview

When HeartLoader is installed and used during integration & testing, the integrator needs to load test Exchange/Portico DUKPT/EMV keys. To facilitate this, the integration package (and not the production package) of HeartLoader includes the KIA (Key Injection Application) that will load on the SIP device. Once the test keys are loaded, the KIA deletes itself and the SIP device reboots to HeartLoader. These test keys need to be loaded to the secure memory of the SIP device by following these steps only. Keys cannot be automated or included with the package because they deal with secure memory.

This step is not required during production as the production DUKPT/EMV keys are pre-loaded in a secure Jeffersonville facility before the HeartLoader package is loaded. Therefore, HSC or integrators downloading a production package of the HeartLoader will not see KIA and will reboot straight to HeartLoader.

#### 9.7.7.2. Get the SIP device ready for key injection

- When KIA is running and the terminal shows the KIA menu.
- Change the COM PORT to USB.
  - Select 2 COM PORT
  - Select 2 USB
- Select “1 START KEY INJECTION”.
- The terminal will display “WAITING FOR COMMAND”.

#### 9.7.7.3. Load keys from PC

- Edit HPAKit\SIP Device\Ingenico\Tools\Whost32\User.cfg and replace default COM4 on the first line with the correct COM port number for the user’s setup. (If Window Control Panel, Device

Manager, Ports, is selected, then the Properties for Ingenico iSC2XX Comm Port window is brought up, then Port Settings, click on Advanced, the current comm port settings is shown.)

- Run the file HPAKit\SIP Device\Ingenico\Tools\TestKeys\inj.bat.
- If the port opens successfully, the key injection application will run.
- Press F5 on the PC Keyboard to select KEY INJECTION.
- The application will the messages below when successful.
  - Loading KTK... OK
  - Loading DUKPT Key... OK
  - \*\*KEYS injected
- Wait for the terminal to reboot and launch the HeartLoader application.

## 9.8. HeartLoader

### 9.8.1. Overview

HeartLoader is a downloader application that communicates to HUDS (Heartland Universal Download System) to download a specific TID and AppID. HeartLoader uses a proprietary HPS protocol over SSL to download application files and application parameters from HUDS.

### 9.8.2. Boot

Each time HeartLoader boots up, it checks to see if there is a new version and upgrades itself. HeartLoader does this by performing a “Heartbeat” message to HUDS with a specific HeartLoader TID/APPID to check for updates. (Parameters used in this process are described further in the configuration section of this document.)

It displays “CHECKING FOR AN UPDATE” on the status line (8), and above that, the HOST, APPID and TID. See settings.txt. Note, due to screen size limitations the HOST (HUDS URL) may be truncated on some devices.

If there is a new version of HeartLoader, it displays “UPDATING” with the total percentage downloaded as it upgrades itself and then displays "UPDATE DOWNLOADED" for 3 seconds before rebooting.

If HeartLoader is up to date, it displays “NO UPDATE AVAILABLE” on status line for 3 seconds then goes to ‘Idle’ or ‘Initializing’ screen.

If error occurs on the heartbeat or update process, it displays the ‘Update Failed’ screen.

### 9.8.3. Idle Screen

At the Idle screen, HeartLoader displays “WAITING FOR COMMAND” and launches its POS LINK using settings in settings.txt. Note that HeartLoader will not go to this screen if the HPA application is also installed.

The following commands are available on this screen:

- Pressing 2, then 3, then CANCEL - Goes to ‘Login Screen’, allowing manual downloads.
- Pressing 5, then 6, then CLEAR - Displays “CLEARED TRY COUNT” and reboots. (SEE UPDITEMAXTRY).
- Pressing 8, then 9, then ENTER - Displays ‘Error Screen’.
- POS may send <StartDownload> request as defined below.

### 9.8.4. Initializing Screen

This screen is displayed when HeartLoader detects a Heartland terminal application such as HPA, this screen is displayed for 3 seconds before launching the application.

The following commands are available on this screen:

- Pressing CANCEL - Goes to ‘LOGIN screen’, allowing manual downloads.

### 9.8.5. Update Failed Screen

If Heartbeat or the Update Download fails, i.e. CANNOT CONNECT or wrong TERMINAL ID: User will see: “UPDATE FAILED” on status line. When on this screen, the user may either press ENTER to continue. Or enter key pattern as described below to get more error details on the ‘Error Screen’.

The following commands are available on this screen:

- Pressing 5, then 6, then CLEAR - Displays “CLEARED TRY COUNT” and reboots. (SEE UPDITEMAXTRY).
- Pressing 8, then 9, then ENTER - Displays ‘Error Screen’.
- Pressing ENTER - Continues to next screen. (either the ‘idle screen’ , or ‘initializing screen’ before launching HPA, if HPA is installed)

### 9.8.6. Error Screen

Error Screen will Display: Title, Current Version, Profile, Error Code, and Error Text, or “NO ERRORS DETECTED”. Due to the limitation of screen size, only a short description will be shown, see the Latest

Downloader vN.N Functional Specification.doc for server and terminal error codes, descriptions, and helpful troubleshooting notes.

The following commands are available on this screen:

- Press any key to return to previous screen.

### 9.8.7. Login Screen

Login screen allows user to initiate manual downloads.

The following commands are available on this screen:

- Pressing CANCEL – Either returns to ‘Idle Screen’ or launches terminal application.
- Enter Login Password. (See ‘Initiating HPA Download’ – ‘Manual Download’ section below.)

### 9.8.8. Configuration

Initial HeartLoader settings are set in a SETTINGS.TXT file (and optionally in STATICIPS.TXT) that are downloaded along with HeartLoader application files while installing HeartLoader. Integrators may edit this file if needed.

- HPA installed: HeartLoader will not enforce the SIPIP (NETWORK CONFIGURATION) settings if more than one application is identified on the device. DHCP and STATIC settings described and listed below will be ignored, and default values will be used. This allows the ownership of network settings to be controlled by the HPA application.
- HPA not installed: HeartLoader will use the SIPIP (NETWORK CONFIGURATION) Settings.txt and manually set parameters. (I.E. DHCP OR STATIC).

#### 9.8.8.1. SETTINGS.TXT

HeartLoader at boot up will read this SETTINGS.TXT file and use the setting options described below:

- HLTID = Terminal ID (For HeartLoader updates)
- HLAPPID = Application ID (For HeartLoader updates)
- HUDSURL = Host URL to use.
- HUDSPORT= Host TCP port to use.
- SIPIP = Network Settings i.e. DHCP, STATIC, or AUTO
- AUTO - (Not yet supported), the SIPIP is obtained by following the steps below in this order: 1. Check current network configuration (by an OS/SDK API) and use if successful. 2. Check TDA.xml

(if Ingenico/RBA) and use if successful. If TDA.xml uses serial, use that for SIPLISTENER and set SIPIP to DHCP.

- DHCP - Use DHCP
- STATIC - For Static IP (Uses STATICIPS.TXT file, see below).
- SIPLISTENER = Port # of POS LINK
- Port # if Ethernet POS link is to be used i.e. SIPLISTENER=12345, uses same IP as was configured at boot and what is displayed on idle "WAITING FOR COMMAND" screen. Configure your POS to communicate with this port and SIP IP.
- Serial POS Link i.e.: SIPLISTENER=SERIAL,1,5,9,5
- Format for Serial Link: "SERIAL,<PORT TYPE>,<FORMAT>,<PORT BAUD RATE >,<INTERNAL SIP COM PORT> "
- PORT TYPE: 1=USB OR 2=RS232
- FORMAT: 1="7E1" 2="7N1" 3="7O1" 4="8E1" 5="8N1" 6="8O1" 7="7N2"
- PORT BAUD RATE: 1="1200" 2="2400" 3="4800" 4="9600" 5="14400" 6="19200" 7="38400" 8="57600" 9="115200"
- PORT NUMBER i.e. 5=USB 0=RS232
- UPDITEMAXTRY = Number of attempts for a HeartLoader upgrade that fails, and does not receive an "up to date" response on the next heartbeat after attempting an update. Minimum =1 Maximum=9

#### 9.8.8.2. Default Settings

If any tag is not present, or if SETTINGS.TXT does not exist on boot up, in addition to setting the following default values, a new SETTINGS.TXT file will be created on the device.

- HLTID / HLAPPID
- See: Application IDs for HeartLoader table below for correct default Application IDs.
- HUDSURL=SSLHPS.PROD.HPSDNLD.NET
- HUDSPORT=8001
- SIPIP=DHCP
- SIPLISTENER=12345



- UPDITEMAXTRY=3
- Notes: Network changes in the manual download screen will not be available after the HPA application is installed. Changes made on the confirmation screen in this mode will cause HeartLoader to save a new SETTINGS.TXT file.
- Unless the SETTINGS.TXT file is updated on HUDS as well, the next upgrade of HeartLoader will use the SETTINGS.TXT file from HUDS and custom settings will be lost.

#### 9.8.8.3. STATICIPS.TXT

This flat file is used to specify the Static IP of the SIP device before any terminal applications are installed such as HPA.

It can contain multiple records, one record per line.

Record format is PIPE '|' delimited: Full SIP serial #|SIP IP Address to use|Subnet Mask|Gateway IP|DNS1|DNS2

EXAMPLE:

15292SC80802174|10.16.36.111|255.255.252.0|10.16.36.1|10.2.23.103|10.2.23.104|

\*|10.16.36.38|255.255.252.0|10.16.36.1|10.2.23.103|10.2.23.104|

If SIP Serial # is a \* (wild card), any serial # is allowed.

HeartLoader reads this file one record at a time from top to bottom, and stops searching when it finds a serial number match or encounters a wildcard '\*' record, and uses that record's settings.

HeartLoader will NOT use the STATICIPS.TXT network settings if another Heartland app such as HPA is installed, as this is only needed for a standalone configuration.

#### 9.8.8.4. Initiating HPA Download

There are two ways to start the HPA download, once HeartLoader has booted up into IDLE state and is displaying "DOWNLOADER MENU". Either the POS can send the StartDownload command containing the download parameters, or the download can be started manually by pressing 1/DOWNLOAD to start the download menu prompting screens.

#### 9.8.8.5. StartDownload

This command will initiate a specific application download from HUDS. Note that the HeartPOS test application supports this command but requires the parameters to be set appropriately.

An example of the StartDownload command is available in the HeartPOS portion of the SDK. Clicking the 'Start Dwnld' button initiates a pop up box where the parameters used by HeartPOS are set/entered. Clicking the OK button initiates sending the command to HUDS.

In the example XML below, HUDSURL is set to the development HUDS server, the application ID (optional) is set to PI8HD30, and the terminal id is set to TESTSIP.

#### 9.8.8.5.1. Request

```
<HL>
  <Version>1.0</Version>
  <Request>StartDownload</Request>
  <HUDSURL>SSLHPS.TEST.HPSDNL.D.NET</HUDSURL>
  <HUDSPORT>8001</HUDSPORT>
  <HUDSTID>TESTSIP</HUDSTID>
  <HUDSAPPID>PI8HD30</HUDSAPPID>
  <DownloadType>FULL</DownloadType>
</HL>
```

#### 9.8.8.5.2. H.8.5.2 Response

```
<HL>
  <Version>1.0</Version>
  <Response>StartDownload</Response>
  <ResultCode>[Result code]</ResultCode>
  <ResultText>[Result text]</ResultText>
  <MultipleMessage>0</MultipleMessage>
</HL>
```

When this command is received, HeartLoader will initiate a full/complete, partial/update or differential download. It will respond with 0/SUCCESS if the command is correct or an error code/error text if the command has errors. See the section [Download Command](#) for more information on differential download.

If the download is successful, the SIP device reboots and no response is sent to the PC.

#### 9.8.8.6. Manual Download

To enter into a manual download:

- Press cancel while initializing is on screen. "Initializing" will show only if HPA is present.
- At Idle, when the device is displaying "DOWNLOADER MENU", press 1/DOWNLOAD to start the download menu prompting screens.

HeartLoader will go into a menu that allows manually entering a URL, port number, terminal ID, application id and start the download. (See HeartLoader v5.X Functional Specification.doc, section 2.7.2, labeled "Downloader Idle Menu" for more detail on manual downloads).

#### 9.8.8.7. After Download

After downloading an application (e.g., HPA), HeartLoader will reboot, then launch the application and HeartLoader will remain in the background.

#### 9.8.8.8. HeartLoader Integration Notes

If an error occurs, i.e. the LABEL 5.X.X.XXXX on HUDS has a HeartLoader application version that does not exactly match the label of the build included, or a zip file that is corrupted or otherwise fails to upgrade to the label version, HeartLoader will keep attempting to load itself until:

- HeartLoader receives an UP-TO-DATE response on a HEARTBEAT within the retry count.
- Exceeds the UPDITEMAXTRY count, (defaults to 3) at which time each subsequent reboot will show “UPDATE FAILED” and the error screen will show “MAX TRIES REACHED”.

The 2 ways to reset the UPDITEMAXTRY count back to 0 again is to update HUDS, then initiate a download from the manual download menu, or to hit 5, 6, then CLEAR keys on update failed or the idle screen.

## 9.9. Heartland Universal Download System (HUDS) Environments

There are two HUDS environments, a development environment and a production environment. Integrators should begin their initial POS development by downloading HPA from the development environment. Once a system is ready for deployment to production, then merchants who have been boarded should then download HPA from the production HUDS environment.

**NOTE:** The HeartLoader application, by default, points to the Production environment URL (SSLHPS.PROD.HPSDNLD.NET), so during development integrators must explicitly configure HeartLoader to use the Development/TEST environment by either setting it in settings.txt, modifying the <HUDSURL> XML element in the <StartDownload> message, or by specifying/modifying the correct URL during the manual download menu.

### 9.9.1. HUDS Development Environment

The HUDS development environment is located at SSLHPS.TEST.HPSDNLD.NET port 8001.

### 9.9.2. HUDS Production Environment

The HUDS production environment is located at SSLHPS.PROD.HPSDNLD.NET port 8001.

### 9.9.3. Application ID and Terminal ID

#### 9.9.3.1. Application IDs for HeartLoader and HPA

\*The HPA terminal ID is unique for each integrator, and is assigned by your POS Support contact.

Terminal	Profile	HPA 5.0
Lane/5000	HPSPROD	PILHD50
	HPSQA	PILHD50Q
	MOCK	PILHD50M
Lane/3000	HPSPROD	PIKHD50
	HPSQA	PIKHD50Q
	MOCK	PIKHD50M

#### 9.9.3.2. HUDS HeartLoader TIDs & AppIDs

Terminal	Profile	HeartLoader 5.0	
		TID	APPID
Lane/5000	HPSPROD	DILDX5X	DILDX50
	HPSQA	DILDX5XQ	DILDX50Q
	MOCK	DILDX5XM	DILDX50M
Lane/3000	HPSPROD	DIKDX5X	DIKDX50
	HPSQA	DIKDX5XQ	DIKDX50Q
	MOCK	DIKDX5XM	DIKDX50M

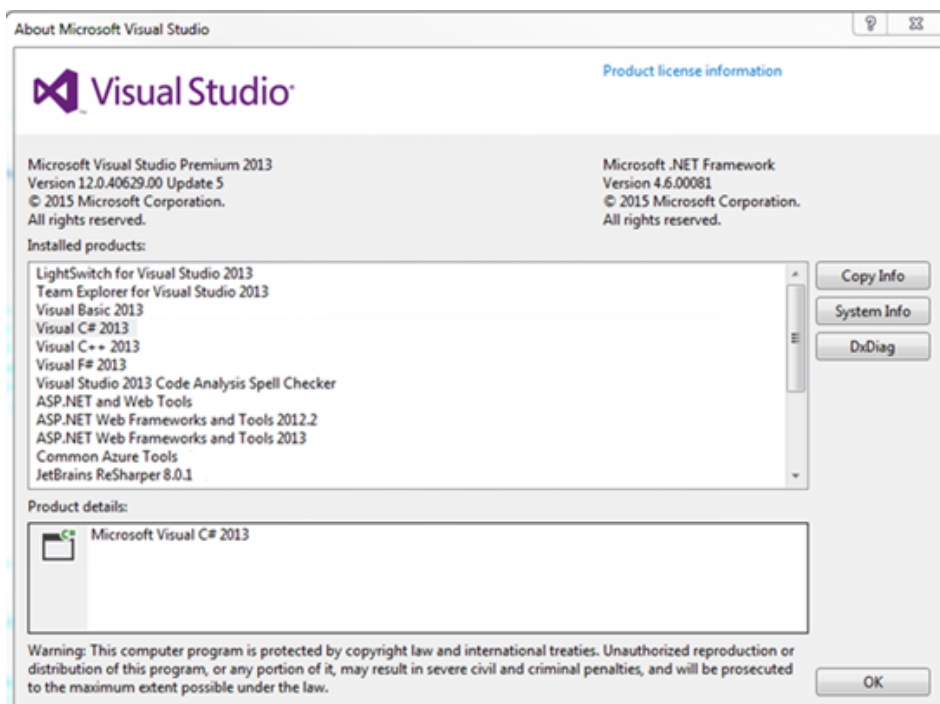
## 9.10. HeartPOS

### 9.10.1. Overview

HeartPOS is a sample (or mock) POS application written in C# that uses the HPA SDK/API to demonstrate how a POS can interface/integrate with a HPA device. It is a real application in the sense that it works in a development environment. It is actively used by HPS developers and QA testers to test the HPA device during development. However, it is not meant to be used in a production environment as it lacks most of the business logic and error processing needed for a true POS application. HeartPOS can be used as a tool or as a sample app by POS integrators when trying to integrate with HPA. POS integrators are encouraged to copy/paste the code from HeartPOS to their POS application.

### 9.10.2. Environment

HeartPOS is written in C# using Visual Studio 2013.



### 9.10.3. Build/Run HeartPOS

Using Visual Studio 2013, you may open the HeartPOS.sln solution and perform Build/Run.

### 9.10.4. Configuration

HeartPOS app uses App.config file for most of the POS configuration settings. Settings can be updated in the file to change the behavior of the HeartPOS app. For example:

- Change the Header and Footer of the virtual receipt
- Set the connection type from POS to SIP
- Set some of the XML elements like the report type, whether to confirm amount on the SIP device or not, etc.
- Open HPAKit\Windows PC\HeartPOS\HeartPOS.sln in Microsoft Visual Studio 2013.
- Open HPAKit\Windows PC\HeartPOS\App.config and configure the POS application. At a minimum:
- To configure for serial communication set:
- In <add key="ECRToSIPConnection" value="1"/> set the "value" to 1.
- In <add key="ECRToSIPSerialPort" value="COM4"/> set the "value" field to correct COM port for the setup.
- To configure for Ethernet communication:
- In <add key="ECRToSIPConnection" value="1"/> set the "value" to 2.
- In <add key="SIPIP" value="10.16.37.5"/> set value to the IP address of the pin pad.
- In <add key="SIPPort" value="12345"/> set value to the port on which the PIN pad is listening.
- To create a token for cardholder the Token request checkbox in HeartPOS configuration panel can be used.
- To do a token sale , token value should be entered in the text box present in HeartPOS configuration panel.
- You may set pre and post forms that will display before and after a sale transaction. For now, HeartPOS is coded to display these pre and post forms (if present) only on a Sale transaction.
- If you do not wish to use forms, use the following blank values.

```

<!-- Pre Payment Forms. Blank = none; -->
<add key="PrePaymentForm1" value=""/>
<add key="PrePaymentForm2" value=""/>
<!-- _____ -->
<!-- Post Payment Forms. Blank = none; -->
<add key="PostPaymentForm1" value=""/>
<add key="PostPaymentForm2" value=""/>
    
```

- If you want forms, you may use sample forms that comes with HeartPOS. Or you may create your own forms using the rules defined in the HPA spec – User Interface section.

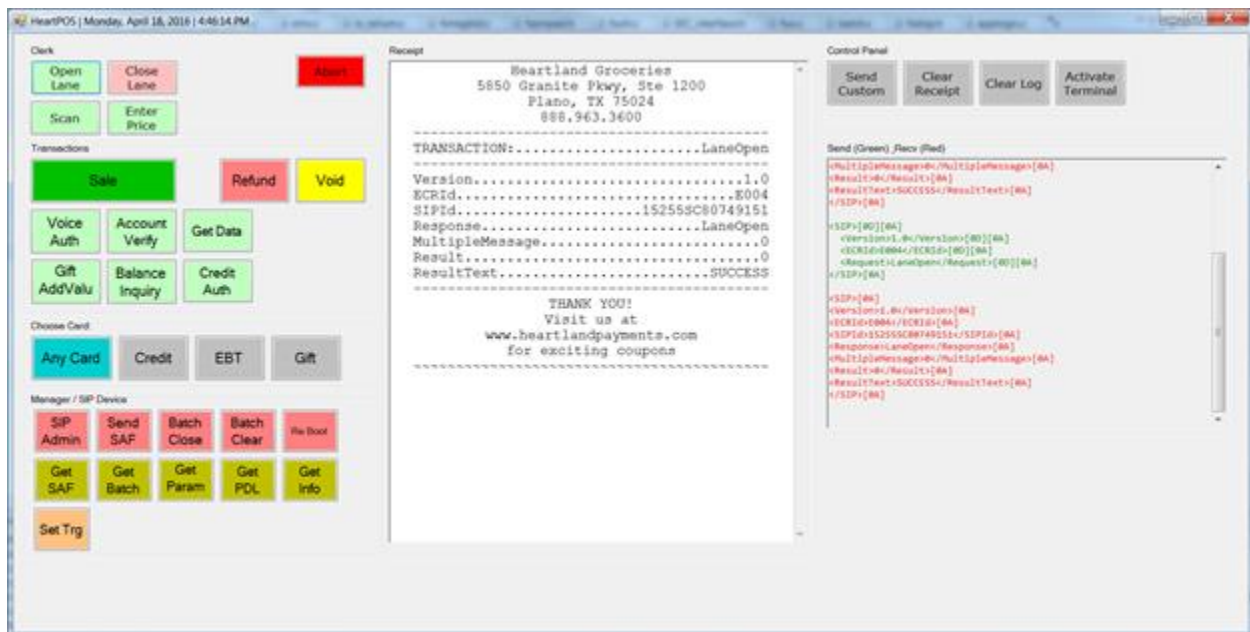
```

<!-- Pre Payment Forms. Blank = none; -->
<add key="PrePaymentForm1" value="Phone.xml"/>
<add key="PrePaymentForm2" value="Fee.xml"/>
<!-- _____ -->
<!-- Post Payment Forms. Blank = none; -->
<add key="PostPaymentForm1" value="Zip5.xml"/>
<add key="PostPaymentForm2" value="Display.xml"/>

```

- Build the HeartPOS application and launch it.

### 9.10.5. HeartPOS UI



### 9.10.6. HeartPOS Usage

When the HeartPOS application runs, it attempts to make a connection to the SIP device using the settings in App.config.

HeartPOS expects the SIP device to be physically connected and running in a Lane Closed state.

It is recommended to start the SIP device first and when it is in a Lane Closed state, start the HeartPOS app.

Use various buttons to perform actions on the SIP device.

Typical use is to open the lane first, scan some items and then perform a Sale, Refund or a Voice Auth.

When you click scan, HeartPOS looks into an Items.xls spreadsheet and randomly picks an item with its price. This is just for demonstration purposes.

Tax for each scanned item is calculated based on the TaxPercent set in the App.config

You may enter a specific price without tax by using “Enter Price” button. This can be used during development when needing a specific amount for a transaction to simulate, such as a partial auth.

Complete the sale on the SIP device by inserting, tapping, swiping, or keying in the card and following any prompts.

If you press the ‘Abort’ button during any transaction flow, that transaction will be canceled and the terminal will display “TRANSACTION CANCELED”. If you want to return to the idle screen then press the ‘Abort’ button again.

**NOTE:** The ‘Abort’ button will not cancel the transaction right away on a PIN Entry screen, only after leaving the PIN Entry screen will the transaction be canceled.

The SIP device will communicate to the HPS host, receive a response, and send an XML response message back to the POS.

HeartPOS unpacks the XML response and prints it on the virtual receipt.

Formatting of the fields is not done in HeartPOS; HeartPOS just prints all the Tags and their Values. Again, this is for demonstration purposes only. In the real POS application, the required Tags/Values would be formatted and presented to the user, printed, stored, etc.

Use Void to void a particular transaction using the Reference #.

Select the card type if you know what card the customer wants to use. Alternatively, set to “Any Card” so SIP prompts the customer. This is all driven by the XML request to SIP.

Use the various Manager buttons to perform Admin functions on the SIP device.

Control Panel’s Send Custom sends the custom.xml to the SIP device. Use this to send a custom XML message to SIP as needed.

Clear Receipt clears the virtual receipt. However, the receipt is saved in a Receipt file, one for each day. You may open it and review the transactions that were run. You need to close the Receipt file before running new transactions in HeartPOS, as it needs control of this receipt file to save.

Clear Log clears the debug window, which shows the XML request being sent in green color and the XML response being received in red color.



### 9.10.7. Transactions Supported

To run the transactions below, select the buttons on the HeartPOS in the order shown in the second column. Every transaction begins in a Lane Open state. When in a Lane Open state, the SIP will display “WELCOME”.

HPA transaction	How to initiate from HeartPOS
Credit Sale	Scan/Enter Price -> Credit -> Sale
Credit Refund	Scan/Enter Price -> Credit -> Refund
Card Verify	Account Verify
Voice Auth	Scan/Enter Price -> Voice Auth (enter a 6 digit approval code)
Credit Adjust	To be implemented.
CPC Edit	To be implemented.
Debit Sale	Scan/Enter Price -> Debit -> Sale
Debit Refund	Scan/Enter Price -> Debit -> Refund
EBT Balance Inquiry	EBT -> Balance Inquiry
EBT CB Sale	EBT -> Sale (Select 2 on HPA)
EBT CB Refund	EBT -> Refund (Select 2 on HPA)
EBT FS Sale	EBT -> Sale (Select 1 on HPA)
EBT FS Refund	EBT -> Refund (Select 1 on HPA)
Voids	Void (Enter reference number to void) <sup>1</sup>
Reversals	Cannot be initiated from HeartPOS
Signatures	Signature Form
EMV Chip Declines	Cannot be initiated from HeartPOS
EMV TC	Cannot be initiated from HeartPOS
Gift Balance Inquiry	Gift -> Balance Inquiry
Gift Sale/Redeem	Gift -> Sale

Gift Reload	Gift -> Add Value
Gift Activate	To be implemented.

1: The Reference number is the GatewayTxnId value sent to the POS in the response for the transaction that is being voided.

## 9.11. HPA ZIP File List and Description

The HPA.zip file contains signed files, image files, and text files.

### Signed Files:

- 8297965000\_829796.P3A – This is the signed HPA executable program.
- 8297965000\_829796.P3P – This is the signed graphic resource data file.
- 8522770000\_WHITELIST.P3P – This is the signed whitelist file.

### Image Files:

- APPLEPAY.JPG – Apple Pay Logo.
- BANNER320.JPG - Default banner file for Lane/3000. Shows Heartland.
- BANNER480.JPG – Default banner file for Lane/5000. Shows Heartland.
- LOGO320.JPG - Default idle logo file for Lane/3000.
- LOGO480.JPG - Default idle logo file for Lane/5000

### Text Files:

- SPC24ENG.DAT – Prompt File for terminals that support 24 columns.
- SPC32ENG.DAT – Prompt File for terminals that support 32 columns.
- CUSTOM.TXT – Prompts used for Edit Form command.

## 9.12. HeartPOS SDK

### 9.12.1. Overview

The HeartPOS SDK makes it easy for a POS developer to integrate with the SIP device. Source code is provided so the POS developer has a choice of making it a DLL or some other component that best suits their needs.

### 9.12.2. HPA Class

The HPA Class provides low-level communication APIs to talk to the SIP device. It provides basic Connect(), Send(), Recv(), Disconnect() calls.

#### 9.12.2.1. Connecting to SIP device

- Use the HPA.HPA() constructor to set the connection type and connection settings.
- ConnectionType supports Serial and Ethernet for now, with USB being a future option.
- The following ConnectionSettings needs to be filled in by the POS.
  - SerialPort. Example: "COM1"
  - UseSerialProtocol – Set it to true if you want to use serial protocol STX, ETX, LRC, ACK, NAK etc. True is recommended.
  - ForcePOSNAK and ForceSIPNAK are used for negative testing. Use 0 for both.
  - IPAddress and IPPort are not supported for now.
  - posDisplay is a call back delegate where the HPA class sends the raw message that is being sent and received. POS can use this data to display in a debug window if needed or stub out the call back.
- Use HPA.Connect() to connect to SIP device.
- It is recommended to use Connect() at the start of the POS application and keep the connection alive while the POS is running. In other words, do not Connect() and Disconnect() for each command.

#### 9.12.2.2. Send command/message to SIP device

- Prepare the XML request message you wish to send to the SIP device.
  - Use HeartPOS.XMLPack() to format your XML message.
- Send to SIP device using the HPA.Send() API

#### 9.12.2.3. Receive command/message from SIP device

- Use HPA.IsReadReady() to check if there is a response from SIP.
- Use HPA.Recv() in a separate thread to receive the response message so as not to block the UI thread.

#### 9.12.2.4. Disconnect from SIP device

- Use HPA.Disconnect() to disconnect from SIP device.
- Use this just before the POS application exits.

### 9.12.3. HeartPOS Class

HeartPOS Class is a sample implementation of the POS application. The useful code here is to see how to pack the XML message and how to unpack the response. This code can be helpful to copy/paste to your POS application code. You may take the entire class and update it as needed.

#### 9.12.3.1. XML Pack

- Use HeartPOS.XMLPack() to pack the XML request command.
- It uses a template file (.xml) in the xml folder. There is one .xml file for each command. Each template has the XML Tags needed for that command. The Tag values are populated by the XMLPack().
- You tell XMLPack() the command you want to pack, and pass in the Tag values via XMLRequestTagValues struct.
- Make sure you pass in all the Tag values required for that command. Otherwise the Tag values will be empty.

#### 9.12.3.2. XML Unpack APIs

- Almost all other XML APIs are for dealing with the XML response.
- You can check if a particular Tag is present, get the value of a particular Tag Value etc.