Specification Update Bulletin No. 56
Second Edition February 2007

CPA Corrections and Changes

This Specification Update Bulletin describes changes to the EMV Common Payment Application (CPA) Specification for Payment Systems. These changes correct errors, clarify ambiguous text, and make functional changes resulting from comments received by EMVCo.

This bulletin is effective immediately.

The changes in this bulletin will be incorporated into version v1.0.b of the CPA Card Type Approval documentation (that is, Test Cases, Card Images, and Implementation Conformance Statement). CPA cards will be tested against the requirements of this bulletin commencing 1 May 2007.

Applicability

This Specification Update Bulletin applies to:

- *EMV Integrated Circuit Card Specifications for Payment Systems Common Payment Application Specification Version 1.0 December 2005*

Related Documents

- Specification Update Bulletin 58 – Editorial Errors in Release 1.0 of the CPA Specifications
- CPA Card Type Approval documentation version 1.0.b.

Description

This Specification Update Bulletin describes changes to the *EMV Integrated Circuit Card Specifications for Payment Systems Common Payment Application Specification*. These changes correct errors, clarify ambiguous text, and make functional changes to the CPA specification in response to comments from readers.

The following summarizes the major changes, corrections, and clarifications. The specific modifications required for these major changes follow this summary:

1) Clarification that personalisation and PUT DATA must support Cyclic Accumulators Data (template 'BF42').

The CPA specification is inconsistent regarding whether update of Cyclic Accumulators Data is supported by personalisation and the PUT DATA command. This bulletin clarifies that the PUT DATA command must support updates to template 'BF42'; that is, updates to a cyclic accumulator value, reference day, and reference date must be supported. This allows issuers to reset the values for the Cyclic Accumulator value, Reference Date, or Reference Day.

2) Clarification regarding handling of variable length data elements within a CPA template tag for PUT DATA and GET DATA.

The padding rules for PUT DATA and GET DATA commands for fixed and variable resource templates are clarified as follows:

The number of bytes filled in the template at personalization time will always remain available for update using PUT DATA. At personalization, these bytes may include filler ('00') bytes.

The application shall accept any PUT DATA (either for a replacement of a resource or for the addition of a new resource) if the total length of the resulting resources in the template is less than or equal to number of bytes filled in the template at personalization. This total length includes the tags, lengths, and values of the resources.

The following is also being clarified:

- Resources in a template update using PUT DATA might come in any order (for example, 'DF02' might be before 'DF01').
- No filler bytes are required in a PUT DATA.
- Filler bytes in the GET DATA response are allowed before, after, or between resources.
- Resources returned in a GET DATA response might be in any order.

3) Correction to description of optional security counters.

The CPA description has an error regarding when a security counter reaches its limit. The security counter behaviour is to be the same when the counter equals the limit as it is when the counter exceeds the limit.

4) Addition of logging of the Profile ID.

The application must be able to log the Profile ID in the Transaction Log. This functionality will be controlled by a new bit in the Application Control that will function similarly to the `Log the ATC´, `Log the CID´, and `Log the CVR´ bits in the Application Control:

- When the bit has the value 0b, the Profile ID is not logged.
- When the bit has the value 1b, the Profile ID is added to the data logged for any transaction that is logged in the transaction log.

5) Correction to handling of P1-P2 in VERIFY command for CPA

In the current specification, the "Offline PIN Verification Performed and PIN Not Successfully Verified" bit in the CVR may not be set correctly if P1-P2 are values not defined in EMV Book 3. It is possible to have the "Offline PIN Verification Performed" bit set without the "Offline PIN Verification Performed and PIN Not Successfully Verified" bit set if P1-P2 are not according to EMV Book 3, but the PIN is wrong.

To correct this, CPA will be updated to comply with the following:

- At the time the card receives a VERIFY command with P1-P2 coded per EMV Book 3, the 'Offline PIN Verification Performed' flag and the 'Offline PIN Verification Performed and PIN Not Successfully Verified' flags in the CVR must both be set to '1'.
- When a PIN verification is successful, the 'Offline PIN Verification Performed and PIN Not Successfully Verified' flag must be set to '0'.
- When PIN verification is not successful, the 'Offline PIN Verification Performed and PIN Not Successfully Verified' flag is not updated and so remains set to '1'.

6) Change to disallow update to Profile Selection File Entry

Some ICC file systems cannot accommodate updates to the Profile Selection File Entry data element, which does not allow the SFI of the Profile Selection File and the number of records in the file to be changed after personalization. CPA is being modified to disallow update to the Profile Selection File Entry data element.

7) Correction to inconsistency between text and flow for incrementing the ATC for CPA

The text increments the ATC after validating the format of the GET PROCESSING OPTIONS command while the corresponding flow also checks for a valid Application Control before incrementing the ATC. The flow is modified to increment the ATC before checking for a valid Application Control.

8) Change to CCI, DKI and Issuer Options Profile Control for Token Authentication Profile

For simplicity of implementation, the CCI and DKI for the Token Authentication Profile (Profile '7E') are to be taken from the Issuer Options Profile Control for the profile rather than being set to fixed values. Furthermore, the Issuer Options Profile Control must also be present for Profile '7E' to allow the application to know the length of the GENERATE AC command data.

9) Correction to inconsistency between text and flow in checking for valid Transaction Date

The check on the validity of the Transaction Date is missing from the text in second GENERATE AC processing for a Cyclic Accumulator in the current cycle, although it is present in the corresponding flow. A new requirement to perform this check is being added to the text.

10) Correction to calculation for Reference Day

The calculation for Reference Day in Annex E is missing the correction for the value of First Day in Cycle, which allows the issuer to start a cycle on any day of the week. An update to Annex E will

indicate that Reference Day = (Transaction Date in Days-First Day in Cycle)/7*7 + First Day in Cycle.

11) Correction to inconsistency between text and flow regarding Transaction Logging for Token Authentication Profile

The text regarding logging of transactions using the Token Authentication profile is inconsistent with the flow for Token Authentication. A requirement is being added to forbid transaction logging for Profile '7E' (Token Authentication).

12) Correction to error in flow for missing Profile Control '7D'

The VLP flow contains an error showing a check for an invalid VLP Profile Control ID. This flow is being corrected to show that VLP Available Funds are decremented by the Amount, Authorised when the Profile Control for Profile '7D' (VLP) exists. If the Profile Control for Profile '7D' does not exist, an error code is returned to the terminal.

13) Correction to inconsistency between text and flow regarding order of accumulator values included in Issuer Application Data (IAD) when VLP and more than two Accumulators are supported

CPA allows for support of more than two Accumulators as additional functionality. If VLP is also supported, the application builds the Issuer Application Data with the VLP and Accumulator values in the following order of priority (if configured to be sent in the IAD):

Accumulator 1 value
Accumulator 2 value
VLP Available Funds value
Accumulator 3 value
Accumulator 4 value
…

14) Change to allow CPA applications the option to reject issuer script commands when a non-issuer script command breaks the MAC chaining that occurs between issuer script commands.

Currently a CPA application is required to process issuer script commands even when commands that are not issuer script commands are received between the issuer script commands. This requirement is removed.

15) Change to accumulate only approved transactions when processing the CSU or the Default Update Counters

Currently the accumulation of the transaction in an Accumulator occurs when processing the CSU or the Default Update Counters with the setting 'Add Transaction to Offline Counters' regardless of whether the transaction was approved or declined. This change causes accumulation of only approved transactions in an Accumulator while counting all transactions (approved and declined) in a Counter.

16) Change to allow checking that the PIN digits in a VERIFY or PIN CHANGE command are in the range from '0' to '9'.

Currently a CPA application is forbidden from checking that the PIN digits in a PIN Block are valid values for a PIN. This check will not be required, but will be allowed

17) Skip PIN-related checks when offline PIN verification is not supported.

This change clarifies that the PIN-related checks are not performed if the application is personalised to not support offline PIN verification.

Proposed Specification Change Notice

The following modifications to the *CPA Specification* apply to the changes summarized above.

1) Clarification that personalisation and PUT DATA must support Cyclic Accumulators Data (template 'BF42').

To allow personalisation and the PUT DATA command to support Cyclic Accumulators Data, please make the following changes to the *CPA Specification*:

Add the following row to the end of Table 21-9 on page 21-10:

'BF42'	*'DF01'-'DF0n', 'DF11'-'DF1n', 'DF21'-'DF2n'*	*Cyclic Accumulators Data: value ('DF0x'), Reference Date ('DF1x'), Reference Day ('DF2x')*	*If any cyclic accumulator is active for any profile personalised in the application and the Issuer wants to set a beginning value, reference date, or reference day.*	*N * 20*	*binary*

Add the following after the first sentence of the first section of Annex I1.1 on page I-2 (above Table I-1):

> "The data elements in Cyclic Accumulator x Data (see Table I-1) may be set at card personalisation or using the PUT DATA command."

Modify the note in Annex I2 at the bottom of page I-7 to the following:

> "NOTE: The Cyclic Accumulator Value, Cyclic Accumulator Reference Date, and Cyclic Accumulator Reference Day in Cyclic Accumulator Data cannot be reset by the CSU that may be contained in the Issuer authorisation response. However, they can be updated with a PUT DATA command to template 'BF42', and a reset is performed automatically when a new cycle begins."

Add the following note after the first paragraph of Annex I3 on Page I-9:

"**NOTE**: The Cyclic Accumulator Reference Date and Cyclic Accumulator Reference Day could also be corrected by a PUT DATA command to template 'BF42'."

Add the following paragraph to the description of Cyclic Accumulator x Data on page L-47:

"The Cyclic Accumulators Data template may be obtained from the application using the GET DATA command with template tag 'BF42' and may be updated using the PUT DATA command."

2) Clarification regarding handling of variable length data elements within a CPA template tag for PUT DATA and GET DATA.

Please clarify the use of PUT DATA and GET DATA with resource templates by making the following changes:

Add a new requirement after Req 12.6 on page 12-8:

"**Req 12.32 (GET DATA response data format for templates):**

The GET DATA response data format shall conform to the following rules:

- *The resources (data objects) can be returned in any order;*
- *Padding shall not be applied within primitive BER-TLV encoded data objects.*
- *Padding shall not be applied outside templates.*
- *Padding may occur within templates, but must be before, after, or between primitive BER-TLV encoded data objects.*
- *The length indicated in the length byte of a padded constructed data object shall include any padding bytes present, since the padding shall only occur within the value field of the constructed data object.*"

Add the following paragraph immediately after the new requirement 12.32:

"The padding bytes have no meaning and can be ignored."

Delete the second sentence (the sentence beginning 'The card returns all data elements ...') in the paragraph following this new requirement 12.32.

Replace Req 18.31 on page 18-29 with:

"Req 18.31 (PUT DATA does not require filler bytes):
For template Tags, the CPA application shall accept PUT DATA commands with no filler bytes in the command data (that is, when the command data only contains the TLV-coded data elements that are to be replaced or added)."

Add the following paragraph and note immediately after the modified requirement 18.31:

"The application may accept filler bytes in a PUT DATA.

NOTE: The issuer cannot rely on the application to accept filler bytes, so the issuer should not include filler bytes in the PUT DATA command."

Replace Req 18.38 on page 18-33 with:

"Req 18.38 (PUT DATA has a template tag in P1/P2):

If P1-P2 contains a template tag, then:

- *The card shall extract each TLV-coded data element (called sub-elements) within the command data. Sub-elements in the command data and already present in the template are for replacement in the template (that is, complete update of the sub-element with the new one, possibly with a different length). Sub-elements in the command data and not already present in the template are for new inclusion in the template. Sub-elements already present in the template and not present in the command data are unchanged.*

- *If the length of the template resulting from:*
  - *Keeping all unchanged sub-elements,*
  - *Updating all sub-elements that are for replacement,*
  - *Adding all sub-elements that are for new inclusion*

  is greater than the reserved length for the template then the card
  - *• shall set the 'Script failed' bit in the PTH to the value 1b*
  - *• shall discontinue processing the Put Data command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6700' (Wrong Length)*

  otherwise, the card shall:
  - *update the template*
  - *increment by one the Issuer Script Command Counter*
  - *respond with SW1 SW2 = '9000'*

NOTE: The card may also check the tag and length of fixed or variable length sub-element before updating the template."

Remove the final paragraph including Req 18.40 from Section 18.8.2 on page 18-34. The paragraph being removed has the following text:

"The PUT DATA command does not require filler bytes in the template data. However, because the command has a length for the command data in addition to the length for each TLV-coded data element, the issuer is allowed to include filler bytes in the command data.

NOTE: EMV uses the value '00' for filler bytes.

Req 18.40 (Filler bytes not required in PUT DATA command):
Filler bytes shall not be required to be sent in the template for a PUT DATA command.."

In the flow on page 18-38, change the text in the lowermost decision diamond from "For each sub-element, L > reserved length for data?" to "Length of updated template > reserved length for template?"

3) Correction to description of optional security counters.

In Annex F1, please replace the third paragraph (beginning 'Initiation of AC Session Key derivation is controlled') though sixth paragraph (beginning 'The SMI Session Key Counter is decremented') with the following text:

"Initiation of AC session key derivation is controlled as follows:

1. If the AC Session Key Counter has reached the AC Session Key Counter Limit (that is, if Counter ≥ Limit), then session key derivation is aborted and the application responds to the GENERATE AC command with SW1 SW2 = '6985'.
2. If the AC Session Key Counter has not reached the AC Session Key Counter Limit, the Counter is incremented and saved in non-volatile memory. The application continues with the AC session key derivation process.

The AC Session Key Counter is reset to zero only when an ARPC is successfully validated.

The AC Session Key Counter Limit shall be less than or equal to 'FF FF'.

SMI session key derivation is only performed if the card receives a script command. Initiation of the SMI session key derivation is controlled as follows:

1. If the SMI Session Key Counter has reached the SMI Session Key Counter Limit (that is, if Counter ≥ Limit), then session key derivation is aborted and the application responds to the script command with SW1 SW2 = '6985'.
2. If the SMI Session Key Counter has not reached the SMI Session Key Counter Limit, the Counter is incremented and saved in non-volatile memory. The application continues with the SMI session key derivation process.

The SMI Session Key Counter is decremented if the first MAC in the script is successfully validated.

The SMI Session Key Counter Limit shall be less than or equal to 'FF FF'."

4) Addition of logging of the Profile ID.

Please make the following changes to require that the application be able to log the Profile ID in the Transaction Log.

Add the following row to Table 15-11 on page 15-74 immediately below the CID row:

Profile ID	if 'Log the Profile ID' in Application Control=1b

Add the following row to Table 17-14 on page 17-70 immediately below the CID row:

Profile ID	if 'Log the Profile ID' in Application Control=1b

In Flow 15-21 on page 15-126 make the following change: The two arrows that currently go to off-page connector "95" instead go to a new decision diamond that says "'Log the Profile ID' in Application Control=1b?" and has an "N" arrow going to off-page connector "95" and a "Y" arrow going to a new box that says "Append Profile ID to current Transaction Log entry". This new box connects to off-page Connector "95".

In Flow 17-30 on page 17-131 make the following change: The two arrows that currently go to off-page connector "S" instead go to a new decision diamond that says " 'Log the Profile ID' in Application Control=1b?" and has an "N" arrow going to off-page connector "S" and a "Y" arrow going to a new box that says "Append Profile ID to current Transaction Log entry". This new box connects to off-page connector "S".

In the row for Optional Card data in Table D-1 on page D-2, add another data element "Profile ID", with description "Profile ID selected for the transaction."

Add a row to the end of Table D-2 on page D-3, with option "Log the Profile ID" and description "This option indicates whether or not the Profile ID is logged."

Add the following row to Table D-5 on page D-7 immediately below the CID row:

Profile ID	if 'Log the Profile ID' in Application Control=1b

Add the following row to Table D-7 on D-8 immediately below the CID row:

Profile ID	if 'Log the Profile ID' in Application Control=1b

In Table D-8 on page D-9, change the value for bit 2 to "0", and change the associated meaning from "RFU" to "Log the Profile ID".

In Table L-10 on page L-18, change the value for Application Control Byte 3, bit 2 to "1", and change the associated meaning from "RFU" to "Log the Profile ID".

In Table K-1 on page K-4, add the following row immediately below the row for tag 'C9', Offline Balance Currency Code:

Profile ID	'CA'	Card

Below Table K-1 on page K-4, change the first NOTE from "Tags in the range 'CA' to 'CF' are RFU for this specification" to "Tags in the range 'CB' to 'CF' are RFU for this specification.

In Table L-57 on page L-65, add the following row immediately below the CID row:

Profile ID	'CA'	1	Application	If the 'Log the Profile ID' bit in Application Control is set to 1

In the dictionary entry for Profile ID on page L-75, change the Tag to 'CA'.

5) Correction to handling of P1-P2 in VERIFY command for CPA

To require setting of the "Offline PIN Verification Performed and PIN Not Successfully Verified" bit in the CVR after the checking of the P1-P2 values in the VERIFY command, please make the following changes to the CPA Specification:

Move the first paragraph, the note that follows this first paragraph, and Requirement 12.13 from Section 12.7.1.1 on page 12-16 to the beginning of Section 12.7.2 on page 12-17.

Modify the text of Requirement 12.13 (which has been moved to Section 12.7.2) to the following:

"*After the card validates the format of the VERIFY command:*

- *If the P1 parameter has the value '00' **and** the P2 parameter has the value '80', then the card shall set the 'Offline PIN Verification Performed' and the 'Offline PIN Verification Performed and PIN Not Successfully Verified' bits in the CVR to the value 1b.*

- *If the P1 parameter has the value '00' **and** the P2 parameter has the value '88' **and** the card supports the Dynamic-RSA implementer-option, then the card shall set the 'Offline PIN Verification Performed' and the 'Offline PIN Verification Performed and PIN Not Successfully Verified' bits in the CVR to the value 1b.*

- *If the P1 parameter has the value '00' **and** the P2 parameter has a value that is supported by the card but is not '80' or '88', then the processing of the VERIFY command is beyond the scope of the CPA specification other than that the 'Offline PIN Verification Performed' and the 'Offline PIN Verification Performed and PIN Not Successfully Verified' bits in the CVR sent in response to the GENERATE AC command shall accurately reflect the results of Offline PIN Verification, as specified in section 9.2.3.1 of the CCD Part of EMV 4.1 Book 3.*"

These changes result in Section 12.7.1.1 beginning with the paragraph saying "The application validates the format of the VERIFY command" followed by Requirements 12.14, 12.15, 12.16, and 12.17 and Section 12.7.2 beginning with "The application sets application indicators to identify that PIN Verification processing has occurred on this transaction" followed by the note from Section 12.7.1.1, and the updated Requirement 12.13.

Replace the text of Req 12.23 on page 12-17 with the following:

"*If the 'Offline Plaintext PIN Verification Supported' bit in the Application Control has the value 0b, then the card shall discontinue processing the VERIFY command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6984' (Command not allowed, referenced data invalidated).*"

Replace the text of Req 12.24 on page 12-17 with the following:

"*If Lc has a value other than '08', then the card shall discontinue processing the VERIFY command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6984' (Command not allowed, referenced data invalidated).*"

Replace the text of Req 12.25 on page 12-18 with the following:

"*If the Transaction PIN Data does not meet **all** of the following conditions:*

- *the Control field of the Transaction PIN Data has the value '2'*
- *the PIN Length field has a value greater than or equal to '4' and less than or equal to 'C'.*
- *the Filler digits of the Transaction PIN Data have the value 'F'*

then the PIN Block format is invalid and the PIN cannot be verified. The application shall discontinue processing the VERIFY command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6984' (Command not allowed; referenced data invalidated).

Otherwise (that is, the PIN Block format is valid), the application shall:

- *decrement the PIN Try Counter by one*
- *compare the Transaction PIN to the Reference PIN.*
  - *If the Transaction PIN does not match the Reference PIN, then PIN verification fails and the application shall respond to the VERIFY command with SW1 SW2 = '63Cx', where 'x' represents the number of PIN tries remaining.*
  - *If the Transaction PIN matches the Reference PIN, then PIN verification is successful and the application shall:*
    - *set the 'Offline PIN Verification Performed and PIN Not Successfully Verified' bit in the CVR to the value 0b.*
    - *reset the PIN Try Counter to the value of the PIN Try Limit.*
    - *indicate successful completion of the command by responding with SW1 SW2 = '9000'.*"

Replace the text of Req 12.26 on page 12-19 with the following:

"*If the P2 parameter is set to the value '88' (Offline Enciphered PIN) and the 'Offline Enciphered PIN Verification Supported' bit in the Application Control has the value 0b, then the card shall discontinue processing the VERIFY command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6984' (Command not allowed; referenced data invalidated).*"

Replace the text of Req 12.29 on page 12-20 with the following:

"*If no challenge from the GET CHALLENGE command immediately prior to the VERIFY command is available, then PIN verification fails and the application shall discontinue processing the VERIFY command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6984' (Command not allowed; referenced data invalidated).*"

Replace the text of Req 12.30 on page 12-20 with the following:

"*After deciphering the Transaction PIN Data, if the recovered data does not meet **both** of the following conditions:*

- *the recovered ICC Unpredictable Number matches the ICC Unpredictable Number sent in the response to the GET CHALLENGE command immediately preceding the VERIFY command,*
- ***and** the recovered Data Header has the value '7F',*

then the application:

- *shall fail PIN Verification*
- *shall discontinue processing the VERIFY command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6984' (Command not allowed; referenced data invalidated).*

Otherwise the application shall continue with verification of the recovered PIN Block."

Replace the text of Req 12.31 on page 12-21 with the following:

"*If the recovered PIN Block does not meet **all** of the following conditions:*

- *the Control field of the recovered PIN block has the value '2'*
- *the PIN Length field of the recovered PIN block has a value greater than or equal to '4' and less than or equal to 'C'.*
- *the Filler digits of the recovered PIN block have the value 'F'*

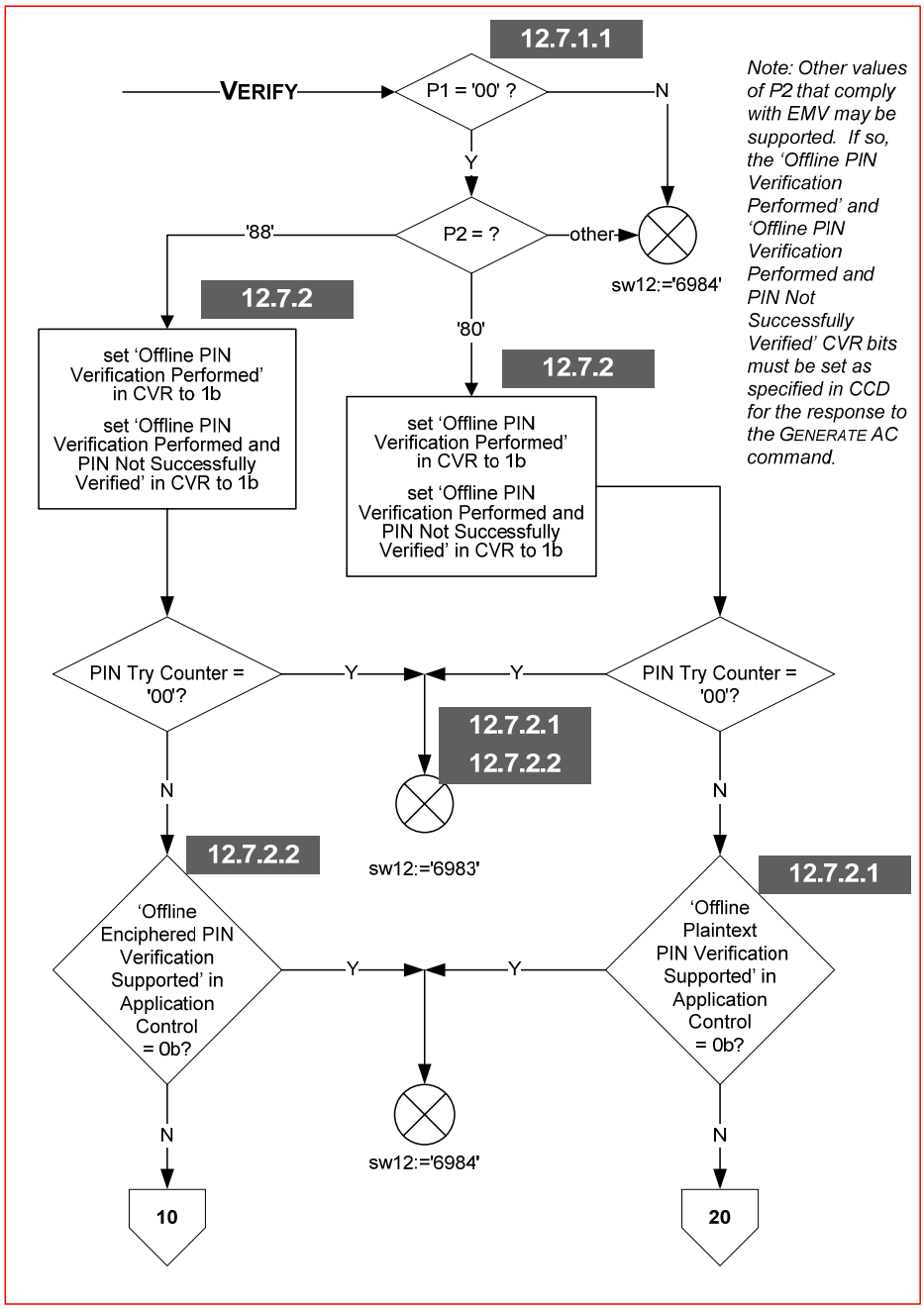
then the PIN Block format is invalid and the PIN cannot be verified. The application shall discontinue processing the VERIFY command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6984' (Command not allowed; referenced data invalidated).

Otherwise (that is, the PIN Block format is valid), the application shall:

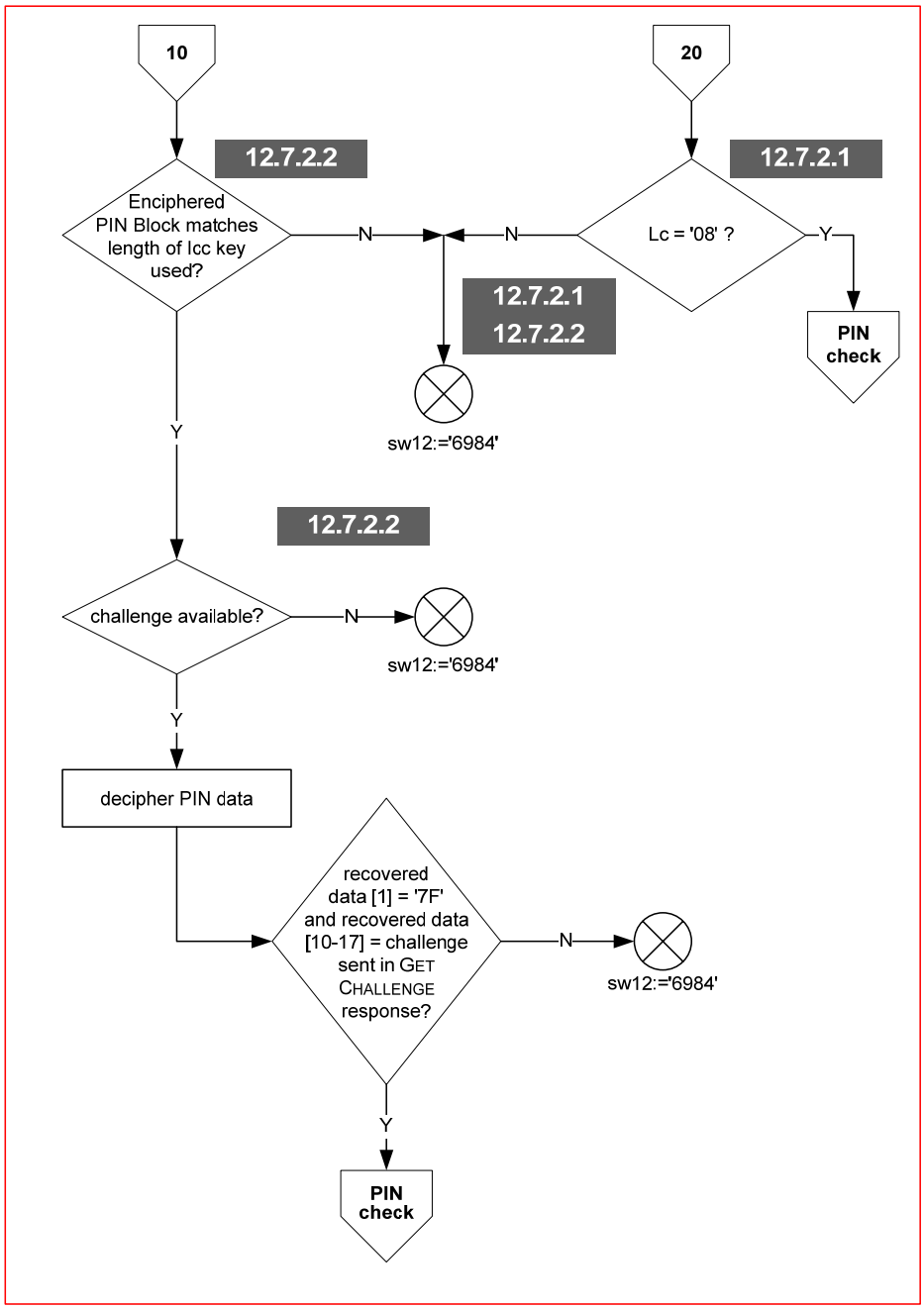
- *decrement the PIN Try Counter by one*
- *compare the recovered PIN to the Reference PIN.*
  - *If the recovered PIN does not match the Reference PIN, then PIN verification fails and the application shall respond to the VERIFY command with SW1 SW2 = '63Cx', where 'x' represents the number of PIN tries remaining*
  - *If the recovered PIN matches the Reference PIN, then PIN verification is successful and the application shall:*
    - *set the 'Offline PIN Verification Performed and PIN Not Successfully Verified' bit in the CVR to the value 0b.*
    - *reset the PIN Try Counter to the value of the PIN Try Limit.*
    - *indicate successful completion of the command by responding with SW1 SW2 = '9000'.*"

Update the VERIFY flow in Figure 12-3 on pages 12-22, 12-23, and 12-24 to the flow on the next three pages:

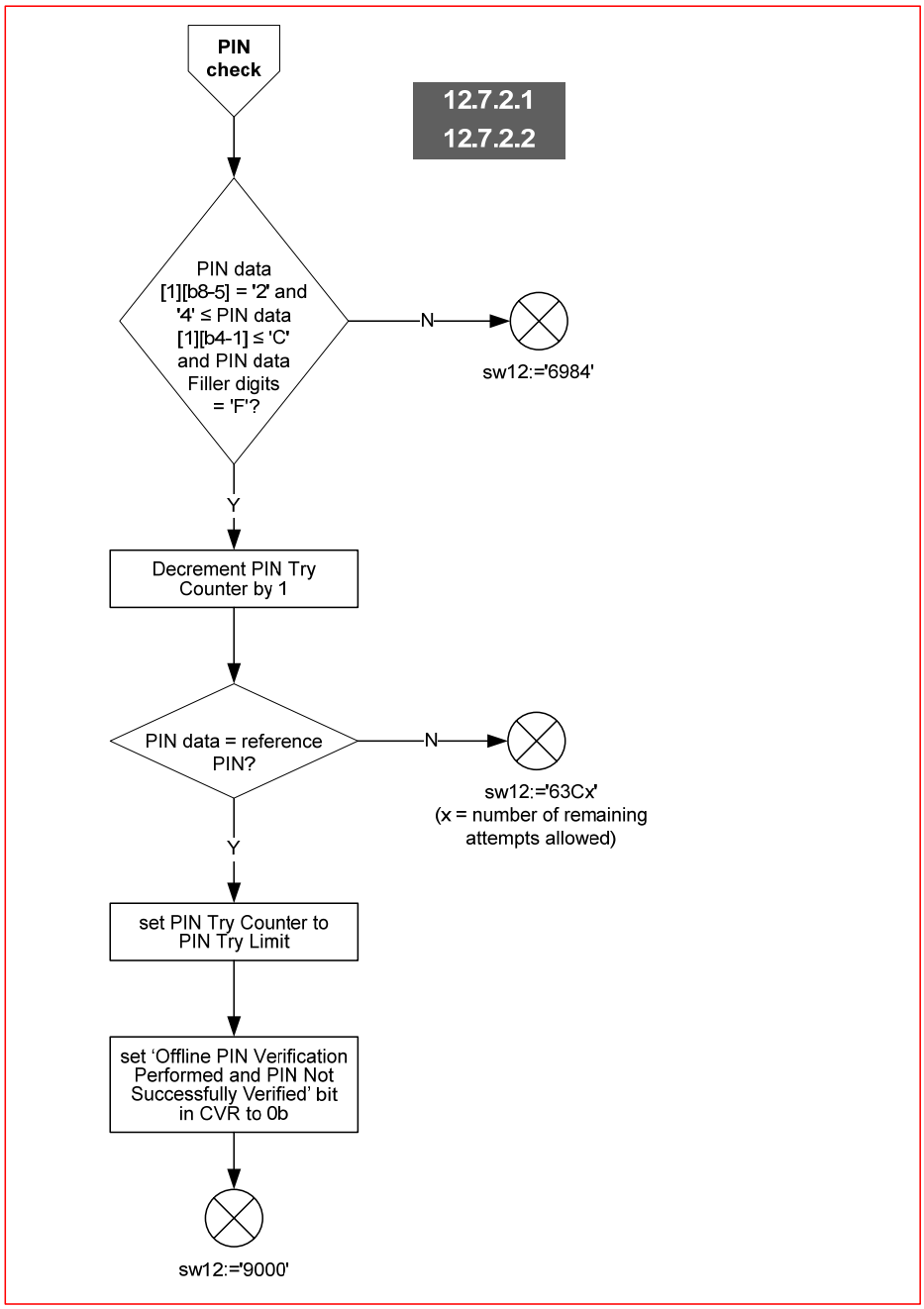
Updated Figure 12-3 VERIFY Page 1
(Page 12-22)



Updated Figure 12-3 VERIFY Page 2
(Page 12-23)



Updated Figure 12-3 VERIFY Page 3
(page 12-24)



6) Change to disallow support for update to Profile Selection File Entry

Please make the following change to the CPA Specification:

In the Profile Selection File Entry row of Table J-1 on page J-2, change the entry in the PUT DATA column to "N".

In the Data Dictionary entry for Profile Selection File Entry on page L-79, delete ", and may be updated using the PUT DATA" from the end of the second paragraph.

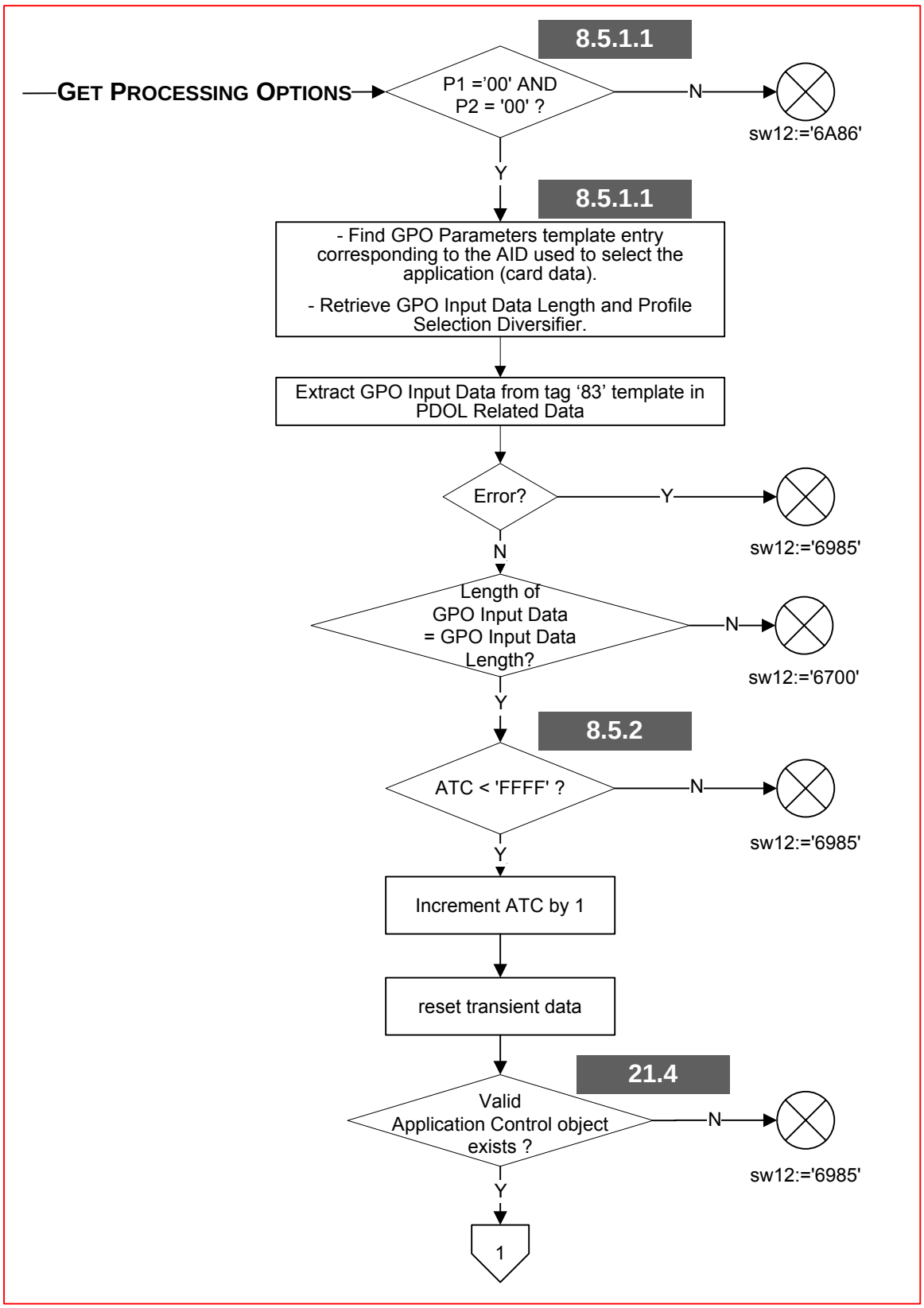
After this second paragraph, add the following note:

> "NOTE: The number of Profile Selection Entries used in Profile Selection depends on the coding of the profile selection logic. If the issuer chooses to reserve space in the Profile Selection File for possible future update to profile selection, the Profile Selection logic may use fewer records than are reserved for the file at the time of personalisation."

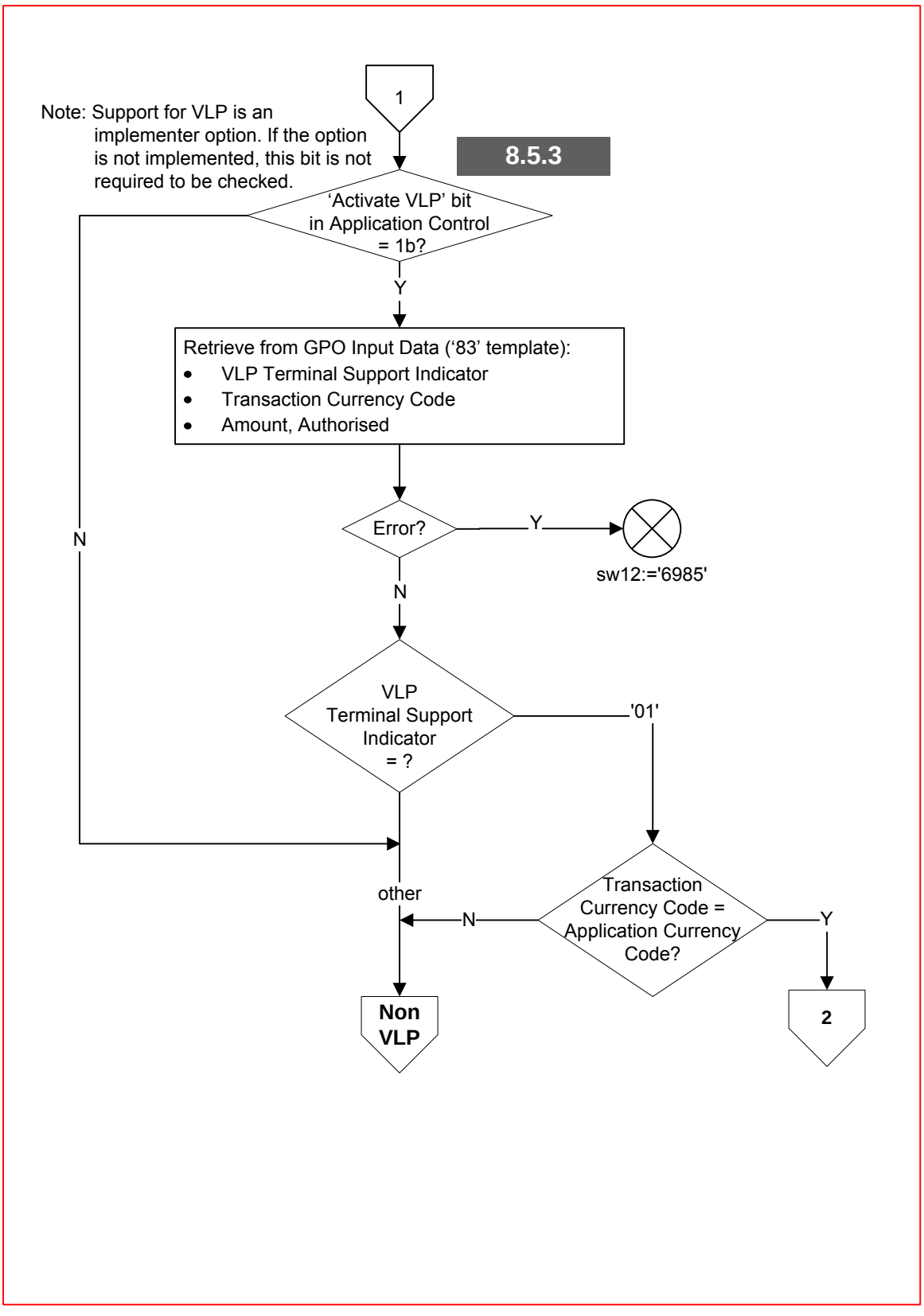
7) Correction to inconsistency between text and flow for incrementing the ATC for CPA

To clarify that the ATC is incremented prior to the check for a valid Application Control, please replace the first two pages of the Initiate Application Processing Flow (Figure 8-1) on pages 8-18 and 8-19 with the flows on the following two pages:

Updated Figure 8-1: Initiate Application Processing Flow Page 1
(Page 8-18)



Updated Figure 8-1: Initiate Application Processing Flow Page 2
(Page 8-19)



8) Change to CCI, DKI and Issuer Options Profile Control for Token Authentication Profile

To indicate that the CCI and DKI for the Token Authentication Profile (Profile '7E') are to be taken from the Issuer Options Profile Control for the profile, please make the following changes to the *CPA Specification*:

Change the CCI and DKI rows of Table 15-9 on page 15-68 to the following to cause the values in Issuer Application Data to come from Issuer Options Profile Control when the Token Authentication profile is selected:

IAD Byte	Description	Value
2	*CCI*	*Set to the value of the Profile CCI in the Issuer Options Profile Control for the transaction ('A5' for CCD-compliant profiles)*
3	*DKI*	*Set to the value of the Profile DKI in the Issuer Options Profile Control for the transaction (issuer-discretionary)*

In Flow 15-7 on page 15-103, change the CCI and DKI entries in the data on the right going into the 'build Issuer Application Data' box to the following:

"CCI, from Issuer Options Profile Control"

"DKI, from Issuer Options Profile Control"

Delete the following text from Requirement 21.64 on page 21-45. With this deletion Issuer Options Profile Control is required to be present when the Token Authentication profile is selected:

"*and the Profile ID selected for the transaction does not have the value '7E',*"

9) Correction to inconsistency between text and flow in checking for valid Transaction Date

Please add the following new requirement to the *CPA Specification* Section 17.5.4.1.6 immediately before Requirement 17.64 on page 17-54 to discontinue checking for the date being within the current cycle if the Transaction Date is not valid:

"**Req 17.89 (Discontinue check if Transaction Date is invalid)**
If the Transaction Date is not valid (see requirement 17.13), then the application shall discontinue processing this check."

10) Correction to calculation for Reference Day

The calculation for Reference Day in Annex E is missing the correction for the value of First Day in Cycle which allows the issuer to start a cycle on any day of the week. To correct this omission, please make the following changes to the *CPA Specification*:

In the flow 17-17.1 on page 17-108, replace the box:

"set Cyclic Accumulator x Reference Day to 1st day of cycle containing Transaction Date in Days"

with two boxes in sequence:

> First box: “compute new Cyclic Accumulator Reference Day”
> Second box: “set Cyclic Accumulator x Reference Day to new Cyclic Accumulator Reference Day”

In Table G-1 on page G-4, add the footnote to Cyclic Accumulator x Reference Day:

> “The value used to represent the Cyclic Accumulator Reference Day depends on the algorithm used for its computation. Such an algorithm is provided in Annex E, but other implementations are allowed. As a consequence, the actual value used by the CPA application to represent the Cyclic Accumulator Reference Day is implementation-specific.”

In Table J-1 on page J-2, add the following footnote to Cyclic Accumulators Data:

> “The value used to represent the Cyclic Accumulator Reference Day within Cyclic Accumulators Data depends on the algorithm used for its computation. Such an algorithm is provided in Annex E, but other implementations are allowed. As a consequence, the actual value used by the CPA application to represent the Cyclic Accumulator Reference Day is implementation-specific.”

On page L-48 Cyclic Accumulator Reference Day, add the following after the description and format for Cyclic Accumulator x Reference Day:

> “The value used to represent the Cyclic Accumulator Reference Day depends on the algorithm used for its computation. Such an algorithm is provided in Annex E, but other implementations are allowed. As a consequence, the actual value used by the CPA application to represent the Cyclic Accumulator Reference Day is implementation-specific.”

Replace the text in Annex E with the new text on the following three pages:

“Annex E Management of Dates in Days

This annex provides algorithms and examples for the management of dates in CPA.

NOTE: Throughout this annex, whole number calculations are described. The result of any division shall be truncated to a whole number.

E1 Date Conversion

The following algorithm could be used to convert a Transaction Date in the EMV format (YYMMDD) into a Transaction Date in Days (an integer).
The **Transaction Date in Days** is the number of days elapsed since an initial date, Day 0.

Converting the transaction date received from the terminal (EMV format) into the transaction date in days is necessary for the following functionality:

- Maximum number of days offline,
- Cyclic Accumulator with weekly cycle.

NOTE: The leap year conversion routine used in this algorithm is limited and will not work in other centuries (that is, where the first two digits for the year are not 20). The algorithm assumes all dates are within the same century (years of the format 20xx).

NOTE: The default ‘Day 0’ used in this algorithm is the 31st of December 1999. Selection of a different initial date is permitted (for example to keep the value of the date in days small, allowing for more efficient calculations). However, the algorithms described in this annex would need to be modified to adjust for the different initial date (day 0).

To compute the number of days elapsed in the **previous years**:

*Number of days in previous years = 365 * YY + (YY + 3) / 4*
(The second term counts the extra days of leap years.)

To compute the number of days elapsed in the **previous months in the current year**:

If MM > 2 and YY is a multiple of 4,
Then Number of days in previous months = (month table entry MM) +1
Else Number of days in previous months = month table entry MM

The month table is then:

{0, 31, 59, 90, 120, 151, 181, 212, 243, 273, 304, 334}

The number of days elapsed since the 31st December 1999, is then:

Transaction Date in Days = [Number of days in previous years]
+ [Number of days in previous months]
+ [Number of days in current month]

If a different (later) initial date is used as ‘Day 0’ the equation becomes:

Transaction Date in Days = [Number of days in previous years]
+ [Number of days in previous months]
+ [Number of days in current month]
– [Adjustment for Day 0 after 31 December 1999]

Examples:
1st January, 2006 (YYMMDD = 060101)
transaction date in days = [365*6 + (6 +3)/4] + [0] + 1 = 2193

27th March, 2012 (YYMMDD = 120327)
transaction date in days = [365*12 + (12+3)/4] + [59 + 1] + 27 = 4470

E2 Computation of Reference Day

When a Cyclic Accumulator uses a weekly cycle, the beginning of a weekly cycle will always be on the same day of the week (for example, Monday). The week day that begins a weekly cycle is specified in the First Day of Cycle element in the Cyclic Accumulator x Control (see Annex L). Since Day 0 (31st of December 1999) is a Friday, the following values are attributed to the First Day of Cycle:

Value	Day of the Week
0	Friday
1	Saturday
2	Sunday
3	Monday
4	Tuesday
5	Wednesday
6	Thursday

Table E-1: Coding of First Day in Cycle

The Cyclic Accumulator **Reference Day** stores the number of days elapsed between the initial date (Day 0) and the first day of the current weekly cyclic period.

If the Transaction Date is in the current cycle (that is, Transaction Date in Days – Reference Day < 7), the Cyclic Accumulator Reference Day does not change.

If the Transaction Date is not in the current cycle (that is, Transaction Date in Days – Reference Day ≥ 7), then a new cycle has to be initiated and the Cyclic Accumulator Reference Day is updated.

If the Transaction Date falls on the day of the week (for example, Monday) specified in First Day of Cycle, then the new Cyclic Accumulator Reference Day is the same as the Transaction Date in Days.

If the Transaction Date falls on any other day of the week, then the new Cyclic Accumulator Reference Day is the day specified by First Day of Cycle immediately preceding the Transaction Date.

This is illustrated in the following picture (the First Day of Cycle is Monday):

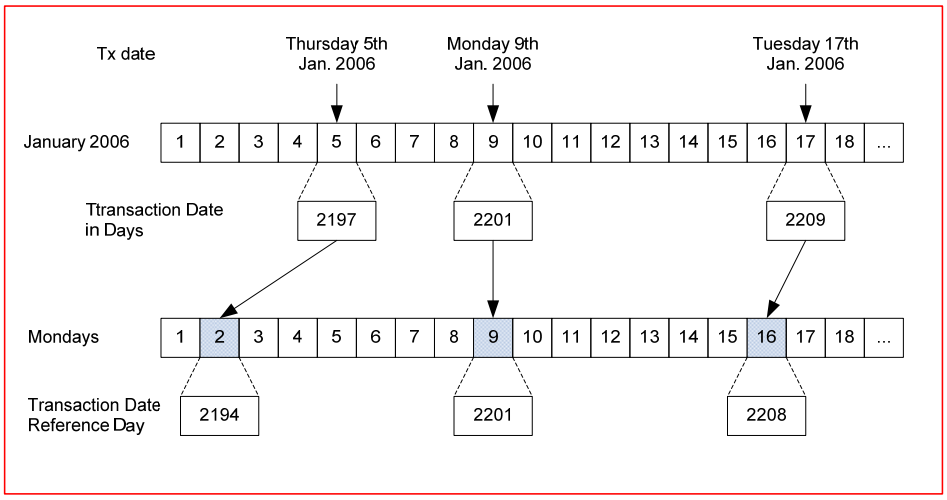


Figure E-1: First Day in Cycle Examples

The equation for calculating a Reference Day from a Transaction Date is the following:

*Reference Day = (Transaction Date in Days – First Day of Cycle) / 7 * 7 + First Day of Cycle*

E2.1 Examples - Week Starting on Monday

For Mondays, First Day of Cycle has value 3.

Transaction Date: Sunday, 1st January 2006 (YYMMDD = 060101)
Transaction Date in Days = 2193
*Reference Day = (2193-3) / 7 * 7 +3= 2187*

Transaction Date: Tuesday, 27th March 2012 (YYMMDD = 120327)
Transaction Date in Days = 4470
*Reference Day = (4470-3) / 7 * 7+3 = 4469*

Transaction Date: Monday, 11th February 2008 (YYMMDD = 080211)
Transaction Date in Days = 2964
*Reference Day = (2964-3) / 7 * 7 +3= 2964*

E2.2 Examples - Week Starting on Sunday

For Sundays, First Day of Cycle has value 2.

Transaction Date: Sunday, 1st January 2006 (YYMMDD = 060101)
Transaction Date in Days = 2193
*Reference Day = (2193 – 2) / 7 * 7 +2= 2193*

Transaction Date: Monday, 11th February 2008 (YYMMDD = 080211)
Transaction Date in Days = 2964
*Reference Day = (2964-2) / 7 * 7 +2= 2963*"

11) Correction to inconsistency between text and flow regarding Transaction Logging not being allowed for Token Authentication Profile

To disallow logging for the Token Authentication Profile, please make the following changes to the *CPA Specification*:

In Section 15.5.8.3 on page 15-73 replace the first two lines of requirement 15.82 with the following:

"*Prior to responding to the GENERATE AC command, if **all** of the following are true:*

- *the 'Log Transactions' bit in the Issuer Options Profile Control has the value 1b,*
- ***and** the Profile Id for the transaction does not have the value '7E'* "

12) Correction to error in flow for missing Profile Control '7D'

To correct the check for an invalid Profile Control ID during VLP processing, please make the following changes to the flow for Requirement 8.5.3 on page 8-21:

- Modify the first decision diamond that currently checks for "VLP Profile Control ID invalid or = 'F'?" to "Profile Control for Profile 7D exists?"

- Change the label on the arrow going from the bottom of this decision diamond to the box saying "Subtract Amount, Authorised from VLP Available Funds" from 'N' to 'Y'.

- Change the label of the arrow going to the right to "SW12:='6985' " from "Y" to "N".

13) Correction to inconsistency between text and flow regarding order of accumulator values included in Issuer Application Data (IAD) when VLP and more than two Accumulators are supported

To correct an inconsistency regarding the order of accumulator values in Issuer Application Data, please make the following changes to the *CPA Specification*:

In the Counters row of Table 15-10 on page 15-70, insert the following bullet after the third bullet:

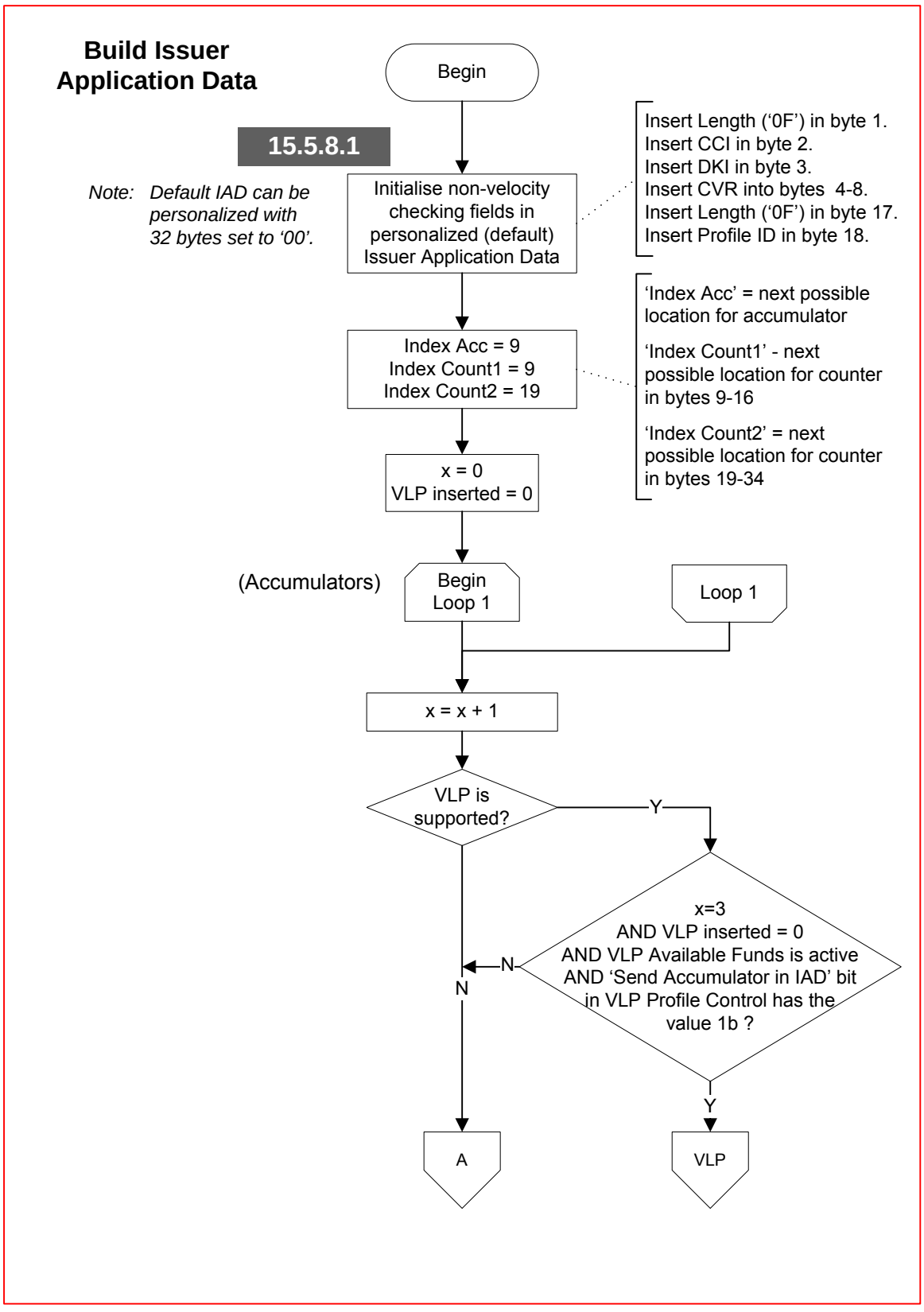
- "*Otherwise, for the lowest value of x for which x is greater than 2 **and** Accumulator x is active for the transaction **and** the 'Send Accumulator x in IAD' bit in the Accumulator Profile Control for Accumulator x has a value of 1b, then Accumulator x (Value or Balance) is sent in Counters bytes 1 - 6.* "

In the 'issuer-discretionary' row of Table 15-10 on page 15-71, add the following bullet after the second bullet in the Value column:

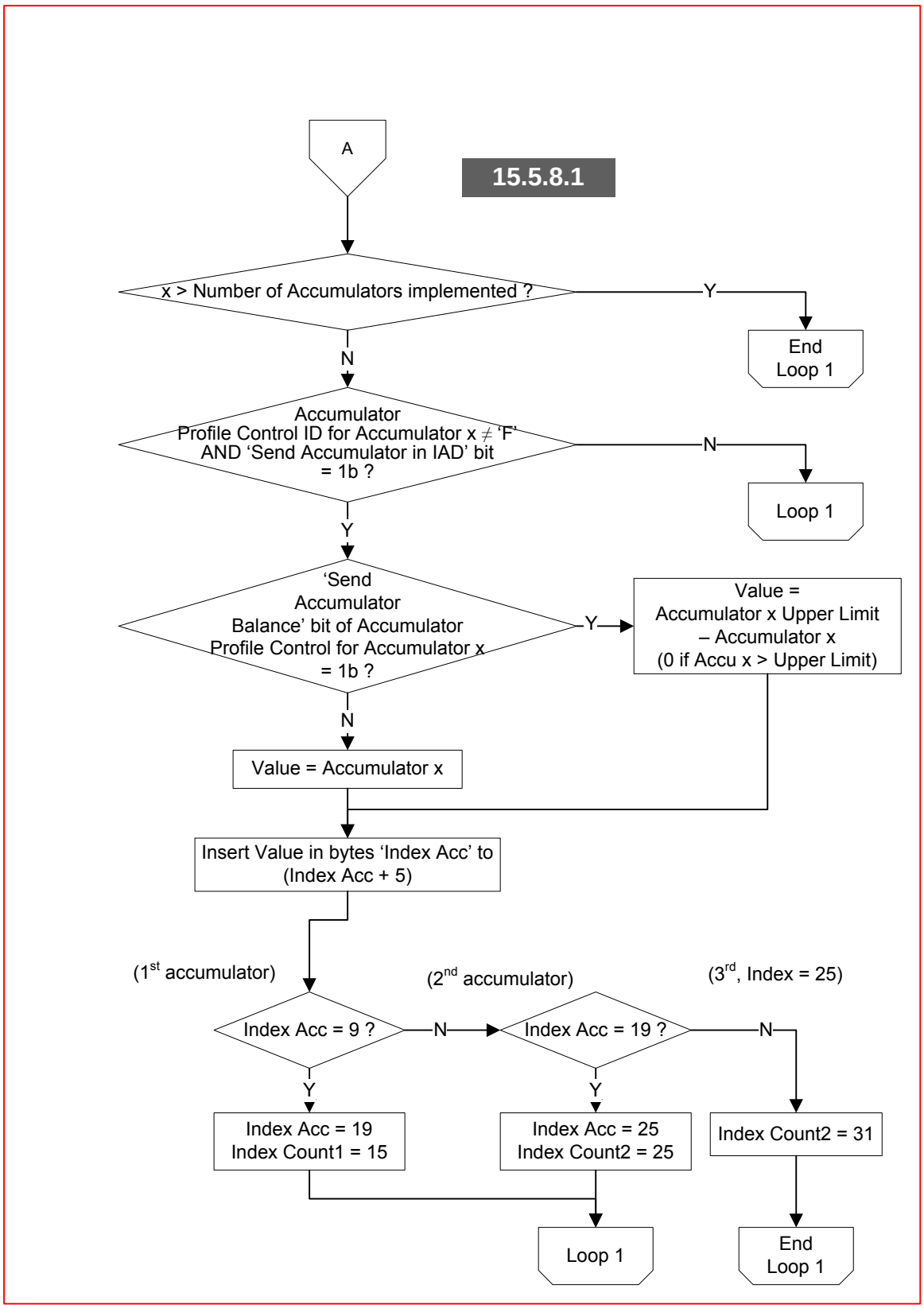
- "*Each Accumulator x (Value or Balance) in order from Accumulator 3 to Accumulator 14 if Accumulator x is active for the transaction **and** the 'Send Accumulator x in IAD' bit in the Accumulator Profile Control for Accumulator x has a value of 1b **and** Accumulator x is not already included in the IAD **and** space for Accumulator x is available in IAD bytes 19-32.*"

To clarify the order in which VLP Available Funds and Accumulator values (or balances) are inserted into the Issuer Application Data, please replace the Build Issuer Application Data Flows (Flow 15-13 through 15-13.2) on pages 15-112 through 15-114 with the flows on the following five pages:

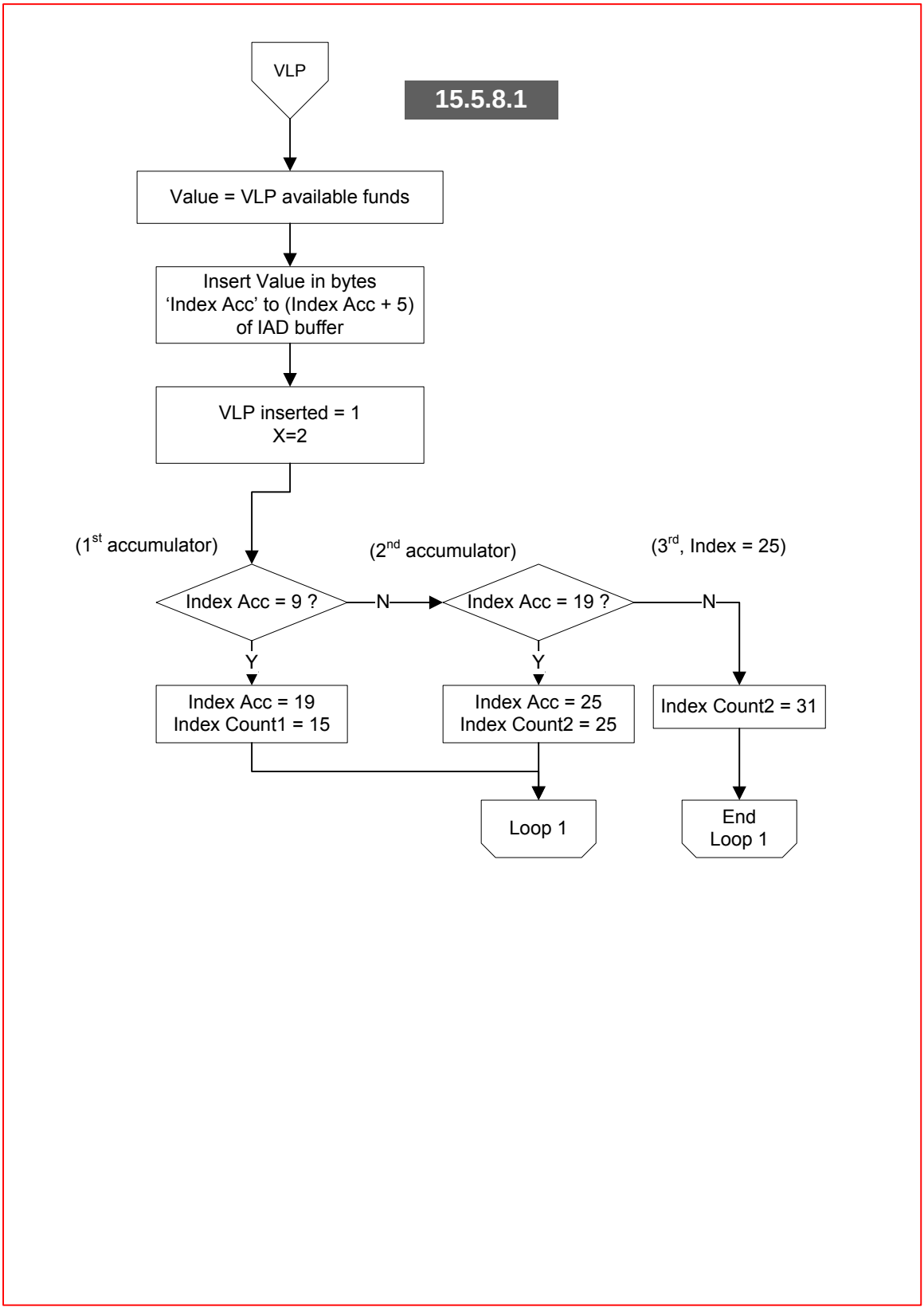
Updated Flow 15-13: Build Issuer Application Data
(Page 15-112)



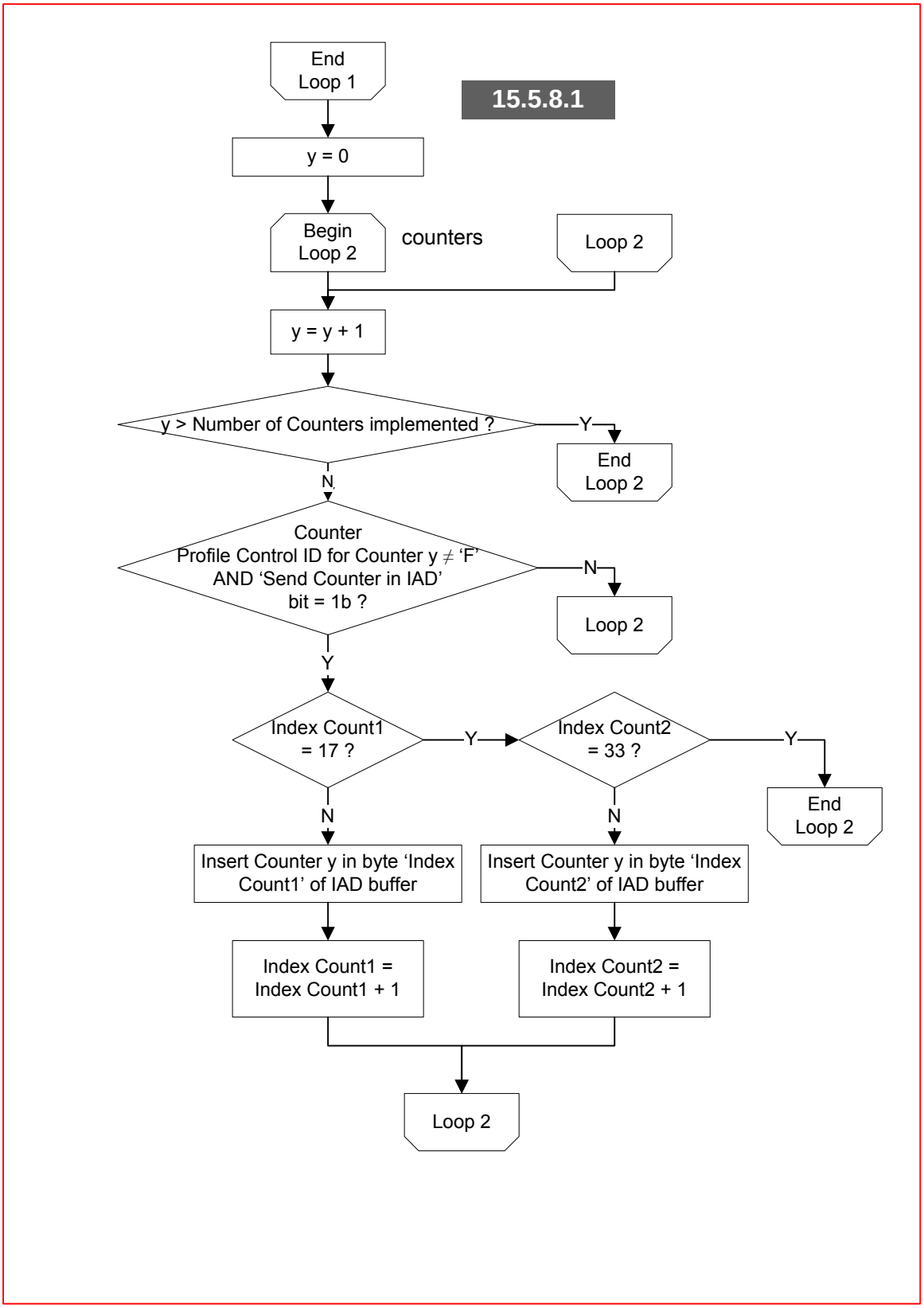
Updated Flow 15-13.1: Build Issuer Application Data
(Page 15-113)



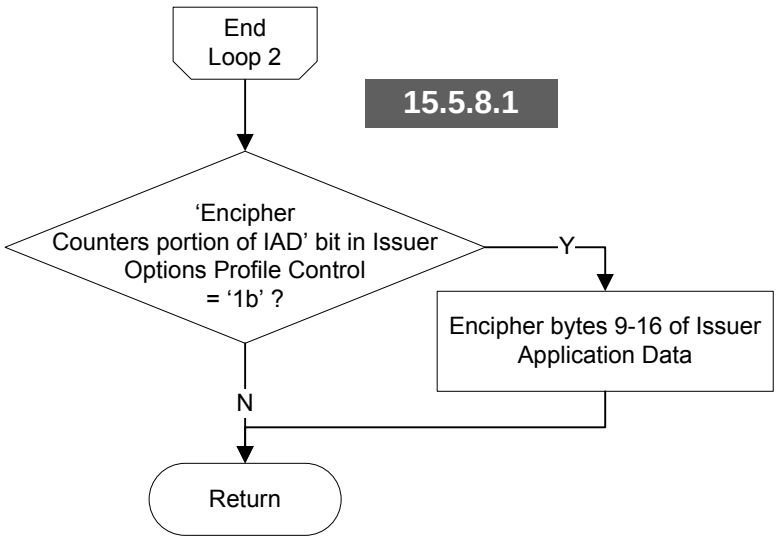
Updated Flow 15-13.2: Build Issuer Application Data
(Page 15-114)



New Flow 15-13.3: Build Issuer Application Data
(After page 15-114)



New Flow 15-13.4: Build Issuer Application Data, continued
(Before page 15-115)



In the Counters row of Table 17-13 on page 17-67, insert the following bullet after the third bullet:

- "*Otherwise, for the lowest value of x for which x is greater than 2* ***and*** *Accumulator x is active for the transaction* ***and*** *the 'Send Accumulator x in IAD' bit in the Accumulator Profile Control for Accumulator x has a value of 1b, then Accumulator x (Value or Balance) is sent in Counters bytes 1 - 6.*"

In the 'issuer-discretionary' row of Table 17-13 on page 17-68, insert the following three bullets after 'in the order shown' in the first paragraph. Please note that only the final bullet is related to this clarification while the first two bullets correct an editorial error that omitted them from the *CPA Specification*:

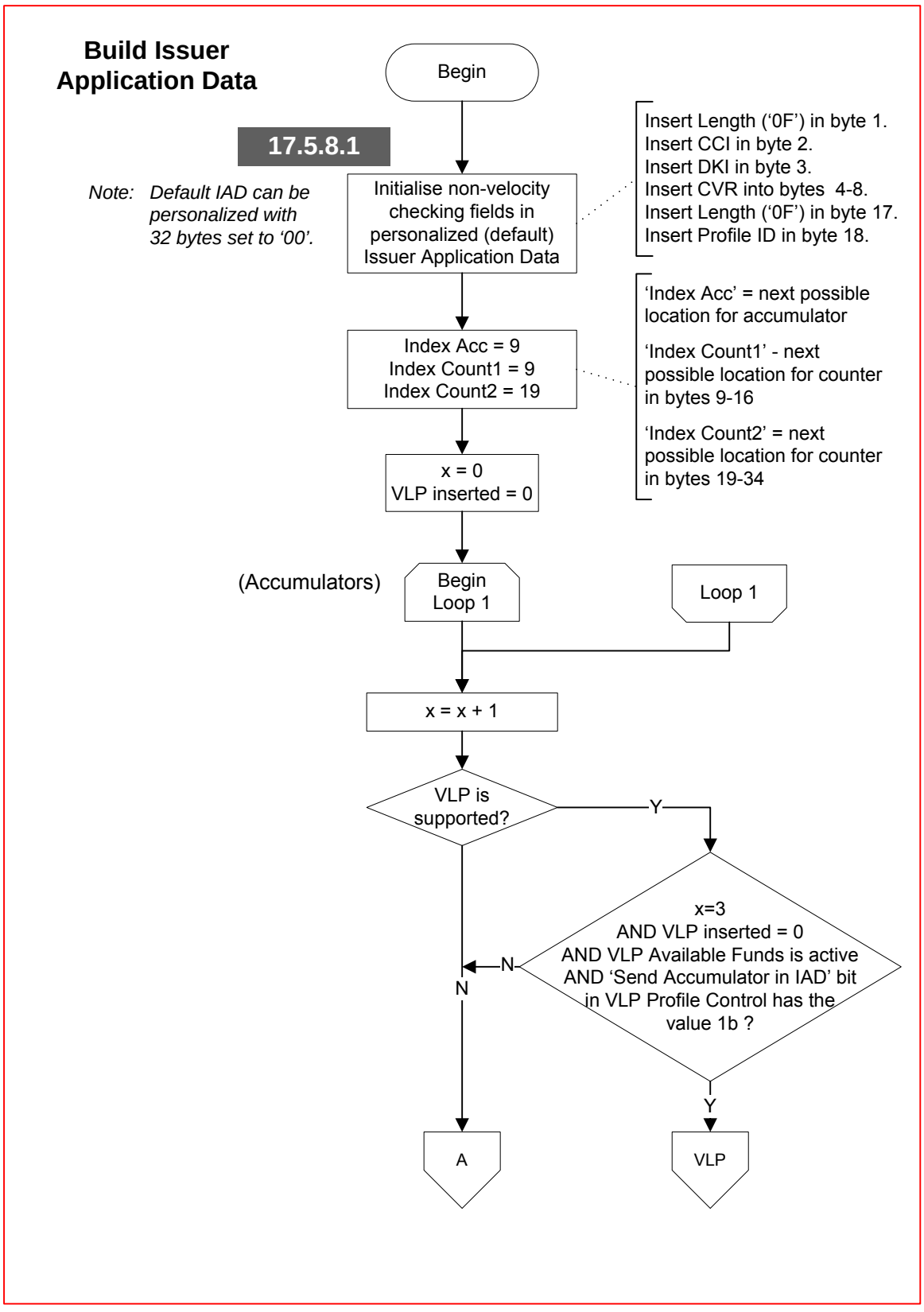
- "*Accumulator 2 if Accumulator 2 is active for the transaction* ***and*** *the 'Send Accumulator in IAD' bit in the Accumulator Profile Control for Accumulator 2 has the value 1b.*

- *VLP Available Funds if VLP is supported* ***and*** *VLP Available Funds is active for the transaction* ***and*** *the 'Send Accumulator in IAD' bit in the VLP Profile Control has the value 1b.*

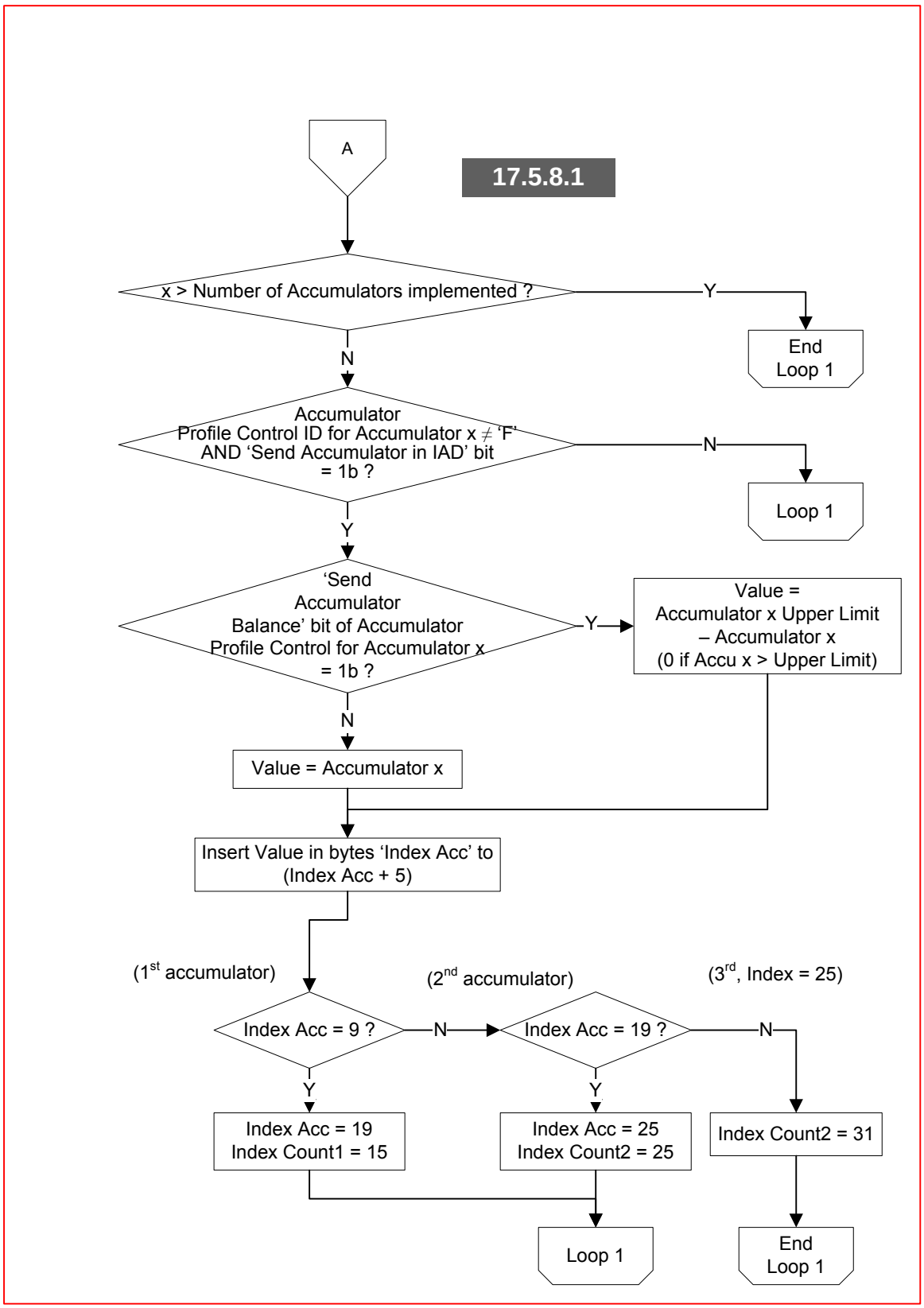
- *Each Accumulator x (Value or Balance) in order from Accumulator 3 to Accumulator 14 if Accumulator x is active for the transaction* ***and*** *the 'Send Accumulator x in IAD' bit in the Accumulator Profile Control for Accumulator x has a value of 1b* ***and*** *Accumulator x is not already included in the IAD* ***and*** *space for Accumulator x is available in IAD bytes 19-32.*"

To clarify the order in which VLP Available Funds and Accumulator values or balances are inserted into the Issuer Application Data, please replace the Build Issuer Application Data Flows (Flow 17-16 through 17-16.2) on pages 17-104 through 17-106 with the flows on the following five pages:

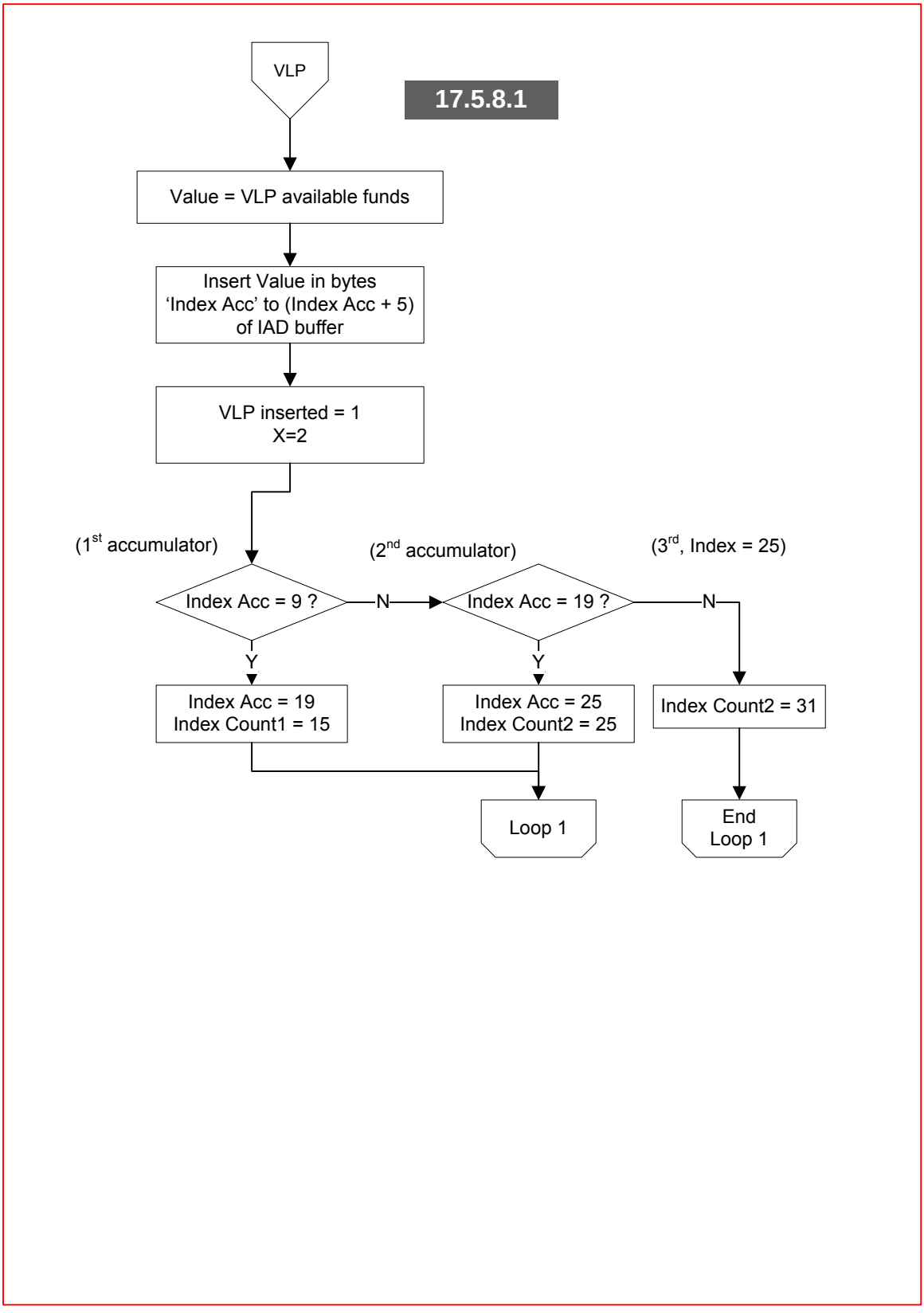
Updated Flow 17-16: Build Issuer Application Data
(Page 17-104)



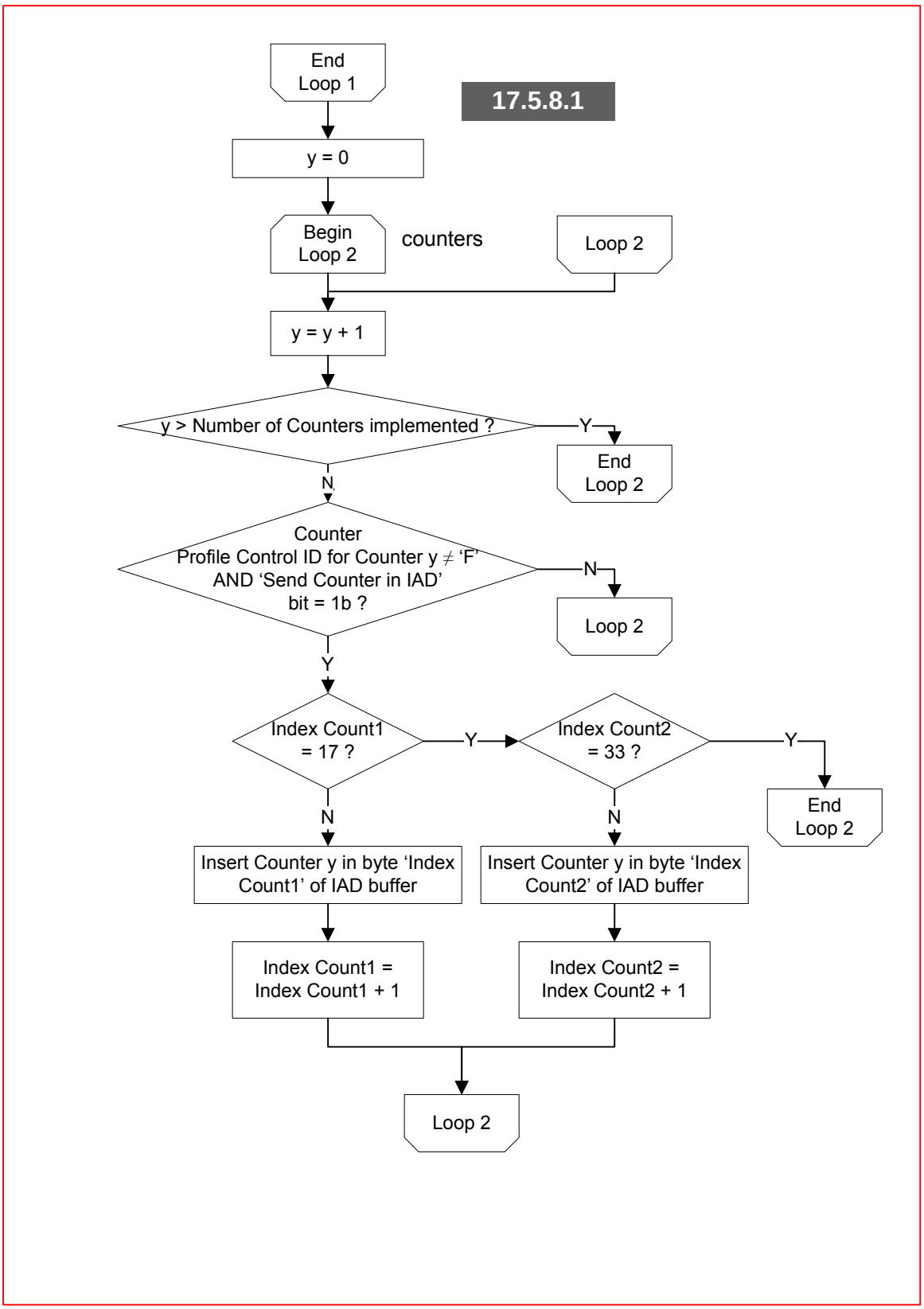
Updated Flow 17-16.1: Build Issuer Application Data
(Page 17-105)



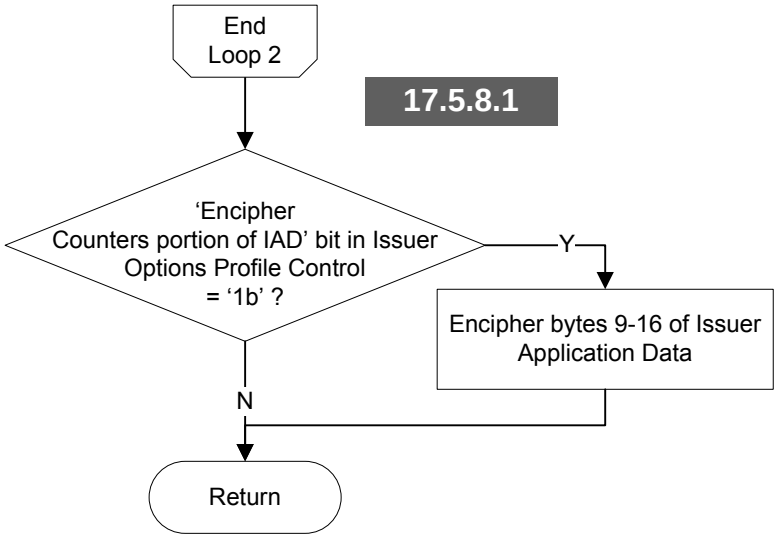
Updated Flow 17-16.2: Build Issuer Application Data
(Page 17-106)



New Flow 17-16.3: Build Issuer Application Data
(After page 17-106)



New Flow 17-16.4: Build Issuer Application Data, continued
(Before page 17-107)



After the second bullet in Section 19.3.1 on page 19-3, add the following as a third sub-bullet:

- "The order of Accumulators (Value or Balance) in the Counters and Issuer Discretionary Data areas of Issuer Application Data is Accumulator 1, Accumulator 2, VLP Available Funds, and additional Accumulators 3 to 14 if the Accumulator is active and specified to be sent in the IAD by Accumulator Profile Control."

14) Change to allow CPA applications the option to reject issuer script commands when a non-issuer script command breaks the MAC chaining that occurs between issuer script commands.

To allow MAC verification to fail when processing issuer script commands received after processing commands in the ONLINE or SCRIPT state that are not issuer script commands and are not a successful second GENERATE AC command, please make the following changes to the *CPA Specification*:

Add the following after the description of the ONLINE state on page 6-3:

> The non-script commands GENERATE AC, GET CHALLENGE, GET DATA and READ RECORD shall be processed as shown in table 6-2 and the command-specific processing described in this specification.
>
> **Req 6.4 (Issuer script commands in ONLINE state)**
> *Issuer script commands shall be processed as shown in table 6-2 and the command-specific processing described in this specification, with the following exception for combinations of script commands and non-script commands received in the ONLINE state. When processing issuer script commands received after processing any commands in the ONLINE state that are not issuer script commands and are not a successful second GENERATE AC command, the application either:*
>
> - *shall process the issuer script command and respond with SW1 SW2 based upon processing results and remain in the current state, or*
> - *shall discontinue processing the issuer script command, shall respond with an SW1 SW2 that indicates an error, should respond with SW1 SW2 = '6985' (Conditions of use not satisfied), and shall remain in the current state.*"
>
> **NOTE**: Non-script commands such as GET CHALLENGE, GET DATA or READ RECORD (both successfully and unsuccessfully processed) and unsuccessfully processed GENERATE AC commands may interrupt MAC chaining; causing subsequent issuer script commands (such as APPLICATION BLOCK, PIN CHANGE/UNBLOCK, PUT DATA, and UPDATE RECORD) in the same transaction to fail MAC verification.

Add the following after the description of the SCRIPT state on page 6-4:

> The non-script commands GET CHALLENGE, GET DATA and READ RECORD shall be processed as shown in table 6-2 and the command-specific processing described in this specification.
>
> **Req 6.5 (Issuer script commands in SCRIPT state)**
> *Issuer script commands shall be processed as shown in table 6-2 and the command-specific processing described in this specification, with the following exception for combinations of script commands and non-script commands received in the ONLINE and SCRIPT states.*

When processing issuer script commands received after processing any commands in the ONLINE or SCRIPT state that are not issuer script commands and are not a successful second GENERATE AC command, the application either:

- *shall process the issuer script command and respond with SW1 SW2 based upon processing results and remain in the current state, or*
- *shall discontinue processing the issuer script command, shall respond with an SW1 SW2 that indicates an error, should respond with SW1 SW2 = '6985' (Conditions of use not satisfied), and shall remain in the current state.*

NOTE: Non-script commands such as GET CHALLENGE, GET DATA or READ RECORD (both successfully and unsuccessfully processed) and unsuccessfully processed GENERATE AC commands may interrupt MAC chaining; causing subsequent issuer script commands (such as APPLICATION BLOCK, PIN CHANGE/UNBLOCK, PUT DATA, and UPDATE RECORD) in the same transaction to fail MAC verification.

Add the following as the third note below Req 18.3 on page 18-9:

NOTE: Non-script commands such as GET CHALLENGE, GET DATA or READ RECORD (both successfully and unsuccessfully processed) and unsuccessfully processed GENERATE AC commands may interrupt MAC chaining; causing subsequent issuer script commands (such as APPLICATION BLOCK, PIN CHANGE/UNBLOCK, PUT DATA, and UPDATE RECORD) in the same transaction to fail MAC verification.

15) Change to accumulate only approved transactions when processing the CSU or the Default Update Counters

To ensure that only approved transactions are accumulated in an Accumulator while allowing all transactions (approved and declined) to be counted in a Counter, please make the following changes to the *CPA Specification*:

In section 17.5.3.1.3, requirement 17.43 on page 17-34, add " ***and*** *'Issuer Approves Online Transaction' bit of the received CSU has the value 1b"* to the first bullet following the "then". The bullet now reads:

- "*For each value of x for which Accumulator x is active* ***and*** *the 'Allow Accumulation' bit in the Accumulator Profile Control for Accumulator x in this profile has the value 1b* ***and*** *'Issuer Approves Online Transaction' bit of the received CSU has the value 1b':*"

In section 17.5.3.1.3, requirement 17.46 on page 17-37, add " ***and*** *'Issuer Approves Online Transaction' bit of the received CSU has the value 1b"* to the first bullet following the "then". The bullet now reads:

- "*For each value of x for which Accumulator x is active* ***and*** *the 'Allow Accumulation' bit in the Accumulator Profile Control for Accumulator x in this profile has the value 1b* ***and*** *'Issuer Approves Online Transaction' bit of the received CSU has the value 1b':*"

In Flow 17-6.4 on page 17-82, add " and 'Issuer Approves Online Transaction' bit =1b'" in the first two diamond boxes. The text in the first diamond box now reads:

> "Accumulator 1 Profile Control ID ≠ 'F' **and** 'Allow Accumulation' bit = 1b **and** 'Issuer Approves Online Transaction' bit = 1b?"

The text in the second diamond box now reads:

> "Accumulator 2 Profile Control ID ≠ 'F' **and** 'Allow Accumulation' bit = 1b **and** 'Issuer Approves Online Transaction' bit = 1b?"

16) Change to allow checking that the PIN digits in a VERIFY or PIN CHANGE command are in the range from '0' to '9'.

Add the following footnote to the end of the first line of Req 12.25:

> "It is allowed, but not required, for an implementation to also check that the values of the PIN digits in the PIN Data are in the range from '0' to '9' as a condition for the PIN block format to be valid."

Add the following footnote to the end of the first line of Req 12.31:

> "It is allowed, but not required, for an implementation to also check that the values of the PIN digits in the PIN Data are in the range from '0' to '9' as a condition for the PIN block format to be valid."

Add the following note next to the first decision diamond in the PIN Check flow on page 12-24:

> "It is allowed to also check that the PIN digits in the PIN Data have values in the range '0' to '9' before comparing with the Reference PIN."

Add the following footnote to the end of the fourth bullet of Req 18.29:

> "It is allowed, but not required, for an implementation to also check for the condition `**and** the PIN digits in the New PIN Block have values in the range from '0' to '9' ´ before allowing update to the Reference PIN."

Add the following note below the symbol containing the text "All filler digits of New PIN Block = 'F'" in the PIN CHANGE/UNBLOCK flow on page 18-28:

> "It is allowed to also check that the PIN digits in the New PIN Block have values in the range '0' to '9' before updating the Reference PIN."

17) Skip PIN-related checks when offline PIN verification is not supported.

Please make the following changes to clarify that the PIN-related checks are not performed if the application is personalised to not support offline PIN verification.

In Req 8.9 on page 8-15 modify the bullet "*PIN Try Counter does not equal 0" with:*

> "*if **either** the 'Offline Plaintext PIN Verification Supported' bit in the Application Control has the value 1b **or** the 'Offline Enciphered PIN Verification Supported' bit in the Application Control has the value 1b, the PIN Try Counter does not equal 0"*

In flow 8-1 on page 8-20, replace the text in the third decision diamond with:

> "('Offline Plaintext PIN Verification Supported' bit = 1b OR 'Offline Enciphered PIN Verification Supported' bit = 1b in Application Control) AND PIN Try Counter = '00'?"

Change Req 15.27 on page 15-29 to the following:

> "*If **both** of the following are true:*
> - ***either** the 'Offline Plaintext PIN Verification Supported' bit in the Application Control has the value 1b **or** the 'Offline Enciphered PIN Verification Supported' bit in the Application Control has the value 1b,*
> - ***and** the 'Offline PIN Verification Performed' bit in the CVR has the value 0b,*
>
> *then the application shall set the 'Offline PIN Verification Not Performed' bit in the ADR to the value 1b.*"

In flow 15-1.1 on page 15-76, replace the text in the second decision diamond with:

> "('Offline Plaintext PIN Verification Supported' bit = 1b OR 'Offline Enciphered PIN Verification Supported' bit = 1b in Application Control) AND 'Offline PIN Verification Performed' bit in CVR = 0b?"

Change Req 15.28 on page 15-29 to the following:

> "*If **both** of the following are true:*
> - ***either** the 'Offline Plaintext PIN Verification Supported' bit in the Application Control has the value 1b **or** the 'Offline Enciphered PIN Verification Supported' bit in the Application Control has the value 1b,*
> - ***and** the 'Offline PIN Verification Performed and PIN Not Successfully Verified' bit in the CVR has the value 1b,*
>
> *then the application shall set the 'Offline PIN Verification Failed' bit in the ADR to the value 1b.*"

In flow 15-1.1 on page 15-76, replace the text in the third decision diamond with:

> "('Offline Plaintext PIN Verification Supported' bit = 1b OR 'Offline Enciphered PIN Verification Supported' bit = 1b in Application Control) AND 'Offline PIN Verification Performed and PIN Not Successfully Verified' bit in CVR = 1b?"

Change the first line of Req 15.30 on page 15-30 to the following:

> "*If the value of the PIN Try Counter is zero **and either** the 'Offline Plaintext PIN Verification Supported' bit in the Application Control has the value 1b **or** the 'Offline Enciphered PIN Verification Supported' bit in the Application Control has the value 1b, then the application shall:*"

In flow 15-1.2 on page 15-77, replace the text in the first decision diamond with:

> "('Offline Plaintext PIN Verification Supported' bit = 1b OR 'Offline Enciphered PIN Verification Supported' bit = 1b in Application Control) AND PIN Try Counter = '00'?"

Add the following new requirement to section 15.5.3.6 on page 15-31:

> **"Req 15.83 (Set CVR PIN Try Counter bits):**
> *If **either** the 'Offline Plaintext PIN Verification Supported' bit in the Application Control has the value 1b **or** the 'Offline Enciphered PIN Verification Supported' bit in the Application Control has the value 1b; then the application shall set the 'Low Order Nibble of PIN Try Counter' bits in the CVR to the value of the low order nibble of the PIN Try Counter, using identical bit settings.*"

In flow 15-1.2 on page 15-77, make the following change:

> The two arrows that currently go to the box "set 'Low Order Nibble of PIN Try Counter' in CVR to PIN Try Counter value'" go to a new decision diamond that says "'Offline Plaintext PIN Verification Supported' bit = 1b OR 'Offline Enciphered PIN Verification Supported' bit = 1b in Application Control?" and has an "N" arrow going to the decision diamond "'Offline Data Authentication Failed on Previous Transaction' bit in PTH = 1b?" and a "Y" arrow going to a box that says "set 'Low Order Nibble of PIN Try Counter' in CVR to low order nibble of PIN Try Counter value'". This box connects to the decision box saying "'Offline Data Authentication Failed on Previous Transaction' bit in PTH = 1b?"

Change Req 17.83 on page 17-65 to the following:

> **"Req 17.83 (Set CVR PIN Try Counter bits):**
> *If **either** the 'Offline Plaintext PIN Verification Supported' bit in the Application Control has the value 1b **or** the 'Offline Enciphered PIN Verification Supported' bit in the Application Control has the value 1b; then the application shall set the 'Low Order Nibble of PIN Try Counter' bits in the CVR to the value of the low-order nibble of the PIN Try Counter, using identical bit settings.*"

In flow 17-19.3 on page 17-114, make the following change:

> The three arrows that currently go to the box "set 'Low Order Nibble of PIN Try Counter' bits in CVR to low order nibble of PIN Try Counter" go to a new decision diamond that says "'Offline Plaintext PIN Verification Supported' bit = 1b OR 'Offline Enciphered PIN Verification Supported' bit = 1b in Application Control?" and has an "N" arrow going to off-page connector "L" and a "Y" arrow going to a box that says "set 'Low Order Nibble of PIN Try Counter' bits in CVR to low order nibble of PIN Try Counter value". This box connects to off-page connector "L".

Change Req 17.84 on page 17-65 to the following:

> **"Req 17.84 (Check PIN Try Limit):**
> "*If the value of the PIN Try Counter is zero **and either** the 'Offline Plaintext PIN Verification Supported' bit in the Application Control has the value 1b **or** the 'Offline Enciphered PIN Verification Supported' bit in the Application Control has the value 1b, then the application shall set the 'PIN Try Limit Exceeded' bit in the CVR to 1b; otherwise, the application shall reset the 'PIN Try Limit Exceeded' bit to the value 0b.*"

In flow 17-19.4 page 17-115, replace the text in the first decision diamond with:

> "('Offline Plaintext PIN Verification Supported' bit = 1b OR 'Offline Enciphered PIN Verification Supported' bit = 1b in Application Control) AND PIN Try Counter = '00'?"