

EMV2000 Integrated Circuit Card Specification for Payment Systems

Version 4.0

Analysis of EMV2000 Changes for Backward Compatibility

Copyright © 2000 EMVCo, LLC. All rights reserved. This document contains proprietary information of EMVCo, LLC. Permission to copy the materials contained herein is granted subject to the following conditions: (i) that all pages of all copies must reproduce this paragraph in full; and (ii) that EMVCo, LLC shall not have any responsibility or liability whatsoever to any other party from the use or publication of the material contained herein.

This document and the information it contains is provided “AS IS”, “WHERE IS” and “WITH ALL FAULTS” and EMVCo, LLC neither assumes nor accepts any liability for any errors or omissions contained in this document. EMVCo, LLC MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND THE INFORMATION IT CONTAINS. EMVCo, LLC SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, INCLUDING THE IMPLIED WARRANTIES OF **MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE**.

WITHOUT LIMITATION, EMVCo, LLC SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES WITH RESPECT TO INTELLECTUAL PROPERTY SUBSISTING IN OR RELATING TO THIS DOCUMENT OR ANY PART THEREOF, INCLUDING BUT NOT LIMITED TO ANY AND ALL IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT OR SUITABILITY FOR ANY PURPOSE WHATSOEVER (WHETHER OR NOT EMVCO, LLC HAS BEEN ADVISED, HAS REASON TO KNOW, OR IS OTHERWISE IN FACT AWARE OF ANY INFORMATION). Users of the information contained in this document are solely responsible for identifying and obtaining any and all patent or other intellectual property licenses that may be needed for products or services developed in connection with this document and the information it contains.

Definition

All changes to Books 1, 2 3 and 4 of EMV 2000 have been analysed for backwards compatibility according to the definition proposed by the EMVCo board. This definition is repeated here.

"An EMV version 3.1.1 approved card shall be accepted and the EMV debit/credit transaction processing successfully executed at an EMV version 4.0 approved terminal. Conversely, an EMV version 4.0 card shall be accepted and the EMV debit/credit transaction processing successfully executed at an EMV 3.1.1 approved terminal - recognizing that the terminal may not support new version 4.0-functionality. Any change to the EMV specifications that adversely impacts these requirements, shall be deemed backward-incompatible."

In the following table, Type 1 compatibility refers to the use of a version 3.1.1 card in a version 4.0 terminal, and Type 2 compatibility refers to the use of a version 4.0 card in a version 3.1.1 terminal.

Considering Book 1, only significant technical changes are treated here; recommendations and editorial changes have been left out for brevity.

Note that some changes impact type approval testing, but do not impact backwards compatibility.

Analysis of EMV2000 Changes for Backward Compatibility

Book 1 - Application Independent ICC to Terminal Interface Requirements

Part I - Electromechanical Characteristics, Logical Interface and Transmission Protocols

Section	Brief description	Type 1	Type 2	Comments
1.1.1.1	Module height increased	Yes	Yes	
1.1.2	Contact and module surface metallisation areas clarified	Yes	Yes	Some 3.1.1 cards are not accepted in terminals having contacts in the 'AFNOR' position
1.3.1	IFD should not have contacts other than C1 to C8	Yes	Yes	Recommendation only, but if followed the problem mentioned above should be eradicated
1.4.1	Terminal operational temperature range reduced	Yes	Yes	
1.4.6	VCC may go slightly negative	Yes	Yes	
1.4.6	VCC transient performance modified	Yes	Yes	
1.4.8	Terminal short circuit resilience clarified	Yes	Yes	
1.4.9	State of signal voltages during terminal powering/depowering clarified	Yes	Yes	
2.1.3.1	New requirements for terminal acceptance of ATR specified (cold reset)	Yes	Yes	
2.1.3.2	New requirements for terminal acceptance of ATR specified (warm reset)	Yes	Yes	
4.3	Limit on the number of characters in the ATR removed	Yes	Yes*	*It is possible (though very unlikely) that a 4.0 ICC returning an ATR having more than 32 characters would be rejected by a 3.1.1 terminal. It is not possible to construct such an ATR using the characters allowed in EMV.
4.3	Terminal shall reject an ICC if there is a parity error in the ATR	Yes	Yes	
4.3.1	Cold and warm ATRs may use different conventions	Yes	Yes*	*It is possible (though very unlikely) that a 4.0 ICC using different conventions in the cold and warm ATRs would be rejected by a 3.1.1 terminal. The requirement for a terminal to support this was not clear in 3.1.1.

Analysis of EMV2000 Changes for Backward Compatibility

Book 1 - Application Independent ICC to Terminal Interface Requirements

Section	Brief description	Type 1	Type 2	Comments
4.3.3.1	Terminal shall accept an extended range of values of TA1	Yes	Yes*	*If a version 4.0 ICC returns TA1 = '12' or '13' in its cold ATR, the ATR is likely to be rejected by a version 3.1.1 terminal. It should fall back to a basic response in the warm ATR, and be accepted, albeit using a slower data transmission speed. This change is important to increase data transmission speeds over the interface.
4.3.3.1	Terminals shall accept any value of TA1 in negotiable mode, and shall use default values for F and D if unable to use the value returned	Yes	N/A	
4.3.3.7	The terminal may accept a wider range of values for TC2	Yes	Yes*	*If a version 4.0 ICC returns a cold ATR with TC2 present and not equal to '0A', a version 3.1.1 terminal may reject it. It should fall back to a basic response in the warm ATR, and be accepted.
4.4	Timing specified for ICC rejection	Yes	Yes	
4.4	Timing modified for deactivation following warm reset	Yes	Yes	
4.4	New terminal requirement introduced for acceptance of minimum 11.8 etu character to character interval during ATR	Yes	Yes	
4.4	Terminal requirement modified for acceptance of maximum 10,080 etu character to character interval during ATR	Yes	Yes	
4.4	Terminal requirement modified for acceptance of maximum 24,000 etu length of ATR	Yes	Yes	
4.4	Timing modified for deactivation following ATR parity error	Yes	Yes	
5.2.2.1	New ICC requirement introduced for acceptance of minimum 11.8 etu character to character interval during T=0 protocol	Yes*	Yes	* Minimal chance of incompatibility dependent on type approval testing technique used – no different from current situation

Analysis of EMV2000 Changes for Backward Compatibility

Book 1 - Application Independent ICC to Terminal Interface Requirements

Section	Brief description	Type 1	Type 2	Comments
5.2.2.1	New terminal requirement introduced for acceptance of minimum 11.8 etu character to character interval during T=0 protocol	Yes	Yes*	* Minimal chance of incompatibility dependent on type approval testing technique used – no different from current situation
5.2.2.1	Terminal deactivation timing specified if max. character to character interval exceeded during T=0 protocol	Yes	Yes	
5.2.2.1	Minimum character to character interval (characters in opposite directions) that the ICC shall be able to receive specified during T=0 protocol	Yes*	Yes	* Minimal chance of incompatibility dependent on type approval testing technique used – no different from current situation
5.2.2.1	Minimum character to character interval (characters in opposite directions) that the terminal shall be able to receive specified during T=0 protocol	Yes	Yes*	* Minimal chance of incompatibility dependent on type approval testing technique used – no different from current situation
5.2.3	Terminal deactivation timing in the event of a parity error modified to accommodate new values allowed for TA1	Yes	Yes	
5.2.4.1.1.1	Clarification of rules for node addressing	Yes	Yes	
5.2.4.2.2	New ICC requirement introduced for acceptance of minimum 10.8 etu character to character interval during T=1 protocol	Yes*	Yes	* Minimal chance of incompatibility dependent on type approval testing technique used – no different from current situation
5.2.4.2.2	New terminal requirement introduced for acceptance of minimum 10.8 etu character to character interval during T=1 protocol	Yes	Yes*	* Minimal chance of incompatibility dependent on type approval testing technique used – no different from current situation
5.2.4.2.2	New ICC requirement introduced for acceptance of maximum CWT + 4 etu character to character interval during T=1 protocol	Yes*	Yes	* Minimal chance of incompatibility dependent on type approval testing technique used – no different from current situation
5.2.4.2.2	New terminal requirement introduced for acceptance of maximum CWT + 4 etu character to character interval during T=1 protocol	Yes	Yes*	* Minimal chance of incompatibility dependent on type approval testing technique used – no different from current situation

Analysis of EMV2000 Changes for Backward Compatibility

Book 1 - Application Independent ICC to Terminal Interface Requirements

Section	Brief description	Type 1	Type 2	Comments
5.2.4.2.2	New terminal requirement introduced for acceptance of first character of a block returned by the ICC during T=1 protocol	Yes	Yes*	* Minimal chance of incompatibility dependent on type approval testing technique used – no different from current situation
5.2.4.2.2	Minimum character to character interval (characters in opposite directions) that the ICC shall be able to receive specified during T=1 protocol	Yes*	Yes	* Minimal chance of incompatibility dependent on type approval testing technique used – no different from current situation
5.2.4.2.2	Minimum character to character interval (characters in opposite directions) that the terminal shall be able to receive specified during T=1 protocol	Yes	Yes*	* Minimal chance of incompatibility dependent on type approval testing technique used – no different from current situation
5.2.4.3	Receiver no longer required to evaluate b4-b1 of PCB of R-blocks	Yes	Yes	
5.2.5	Character repetition forbidden when T=1 used	Yes	Yes	
5.2.5.1	Terminal action and timing in the event that the ICC does not respond within BWT or WTX modified	Yes	Yes	
5.2.5.1	Terminal action and timing in the event that CWT exceeded when receiving characters from the ICC modified	Yes	Yes	
5.2.5.1	ICC shall remain in reception mode if it does not receive a valid response to a block sent twice	Yes	Yes	

Book 1 - Part II – Files, Commands and Application Selection

Section	Brief description	Type 1	Type 2	Comments
7.3.4	Application Label made mandatory	Yes*	Yes	*A 3.1.1 card which does not have Application Label in the FCI may be rejected by a 4.0 terminal. Risk is felt to be small since all known cards include the Application Label.
8.3.2	Fallback to selection by list of AIDs added in cases of failure	Yes	Yes	

Analysis of EMV2000 Changes for Backwards Compatibility

Book 2 - Security and Key Management

Section	Brief description	Type 1	Type 2	Comments
5.1 and 6.1	Removal of Exponent 2	Yes	Yes	
5.1 and 6.1	Issuer Public Key Modulus Length	Yes	Yes	
5.1 and 6.1	SDA Tag List limited to only contain the AIP	Yes*	Yes	* Version 3.1.1 ICCs containing an SDA Tag List with tags other than '82' will fail off-line data authentication in version 4.0 terminals. Risk is felt to be small because no known cards use SDA Tag List.
6.1	ICC and PIN Encryption Public Key Moduli Length	Yes	Yes	
6.6	Combined DDA/AC Generation	Yes	Yes	Combined DDA/AC generation is optional for both the ICC and the terminal. Version 3.1.1 ICCs will work in version 4.0 terminals with option because optional feature will not be attempted. Version 4.0 ICCs with option will work in version 3.1.1 terminals because optional feature will not be attempted.
11.1.2	Encryption requirements for Offline Enciphered PIN at non-integrated PIN pads changed.	Yes	Yes	
A1.3	Application Cryptogram and Issuer Authentication	Yes	Yes	The methods provide guidance to issuers for the implementation of these functions, without excluding issuer proprietary methods.
A1.3	Session Key Derivation Method	Yes	Yes	The methods provide guidance to issuers for the implementation of these functions, without excluding issuer proprietary methods.
A1.4	Master Key Derivation Method	Yes	Yes	The methods provide guidance to issuers for the implementation of these functions, without excluding issuer proprietary methods.
B1.1	Removal of Single-DES	Yes	Yes	The 1998 break of single-DES has triggered a massive migration to double-length key triple-DES within the financial industry.

Analysis of EMV2000 Changes for Backward Compatibility

Book 3 – Application Specification

Section	Brief description	Type 1	Type 2	Comments
1.4	'Generally' deleted from statement on no TLV encoding of DOL data.	Yes	Yes	Clarification
1.4	Padding of data elements clarified.	Yes	Yes	Correction of error.
2.1	The behaviour for Le=00 is clarified.	Yes	Yes	Clarification
2.3.5	The footnotes under the Status word table deleted	Yes	Yes	Clarification
2.3.5	Statement prohibiting verification of RFU data added.	Yes	Yes	Clarification
2.5.5	Bits in Cryptogram Information Data assigned for Payment Specific Cryptogram	Yes	Yes	Bits were previously RFU.
2.5.10.2	Explanation that the values of 01 and 02 for P2 are reserved for the payment schemes added.	Yes	Yes	Editorial clarification.
3.4	Clarification of required and optional data edits.	Yes	Yes	Editorial
6.3 and elsewhere	Combined DDA/Generate AC added as an option.	Yes	Yes	See Book 2 comments
6.4.2	Note regarding cashback deleted..	Yes	Yes	Editorial clarification.
6.5	Clarification of 'unrecognized CVM' role in terminal	Yes	Yes	Clarification
6.5.1	The first bullet in the list split into 2	Yes	Yes	Clarification
Annex A, D and E	Tag number for Issuer URL Data Object changed.	Yes*	Yes*	Alignment with ISO 7616. * Tag is not currently used.
Table A-2	Tag '52' deleted	Yes	Yes	Tag is no longer used.
B1.1	A note from ISO 7816-4 on the usage of '00' and 'FF' between TLV-coded data objects has been included.	Yes	Yes	Clarification
Annex C1	AIP Byte 1 bit 3 clarified.	Yes	Yes	Clarification

Analysis of EMV2000 Changes for Backwards Compatibility

Book 4 – Cardholder, Attendant, and Acquirer Interface Requirements

Section	Brief description	Type 1	Type 2	Comments
2.3.4.5	Clarification of ‘No CVM Required’	Yes	Yes	EMV Technical Bulletin #8, July 2000
2.3.7	Clarification of requirement for advice message support.	Yes	Yes	Precision
2.3.7	Combined DDA/Generate AC	Yes	Yes	See Book 2 comments.
2.3.9	Statement regarding network support for script length of 24 bytes deleted.	Yes	Yes	
2.5.2	Clarification of when a voice referral is required.	Yes	Yes	Clarification
3.4	Requirement for real time clock accuracy relaxed	Yes	Yes	Relaxed requirement – No card impact
3.5	Example of printing the PAN on receipt deleted.			
5	Clarification of software upgrade requirements.	Yes	Yes	Clarification
6.2	Possibility of multiple PIN Pad secret keys supported	Yes	Yes	Clarification
6.2	Clarification of requirement for display of error message during load of Certification Authority Public Key.	Yes	Yes	Clarification
8.2.3	Clarification of text regarding transmission of the reversal	Yes	Yes	Clarification.
Annex A1	Terminal Risk Management	Yes	Yes	
Annex D2.1	Requirement reworded to ‘The power supply should comply with relevant National safety regulations’.	Yes	Yes	Recommendation