EMV®
Interoperability Working Group

Issues List

Version 6.3
September 2017

Ref. IWGVR039-V01

Legal Notice

The EMV® Specifications are provided "AS IS" without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these Specifications. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THESE SPECIFICATIONS.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to the Specifications. EMVCo undertakes no responsibility to determine whether any implementation of the EMV® Specifications may violate, infringe, or otherwise exercise the patent, copyright, trademark, trade secret, know-how, or other intellectual property rights of third parties, and thus any person who implements any part of the EMV® Specifications should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, the Specifications may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries. Any party seeking to implement these Specifications is solely responsible for determining whether its activities require a license to any such technology, including for patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights in connection with the EMV® Specifications.

Contents

1 Interoperability Issues

1.1 Summary of Findings and Status

Of the interoperability incidents reported to EMVCo, the IWG has determined that few of the problems are true EMV interoperability issues that could have been prevented either by clarifications to the EMV specifications or the related EMVCo Type Approval testing process.

As of September 2017, with ninety-one total reported incidents, only one of the earlier issues required a change to the EMV specifications. In a number of the reported incidents, EMVCo has published application notes, bulletins, or best practice guides to help prevent interoperability problems as indirect consequences to resolutions. In other incidents, EMVCo test cases have been added or updated so that similar incidents might be prevented in the future.

Many of the reported issues were the result of:

- Improper behavior of chip devices deployed prior to the establishment of EMVCo approvals
- Member card personalization and terminal implementations
- Payment system and network-related incompatibilities

All these types of incidents, reported to EMVCo, were (and will continue to be) transferred to the appropriate payment system for resolution. For the most effective problem management of interoperability issues, incidents are best reported directly to the payment system. The primary reasoning for this approach is because:

1. A majority of the problems, as evidenced by the incidents initially reported to EMVCo, are not directly or indirectly consequential to EMV specifications or EMVCo type approval test cases.
2. The resolution of almost all the reported problems is most effectively implemented by the payment systems in conjunction with its affected Members directly.

Should any actions need to be taken by EMVCo, or should the issue be likely to have global impact, payment systems have been requested to forward these requests along with the problem background to the IWG.

2 Explanation for Problem Impact Classification

In order to better depict problem severity, all the issues have been given a classification of Red/Yellow/Green (or High Medium Low) in three categories – Transaction Result, Volume and Field Implementation. The classification for each reported issue can be found in each issue summary in Section 3. The levels and characteristics of each category are:

1. Classification by Impact of Transaction Result

🔴 =HIGH TRANSACTIONS **ABEND** OR RESULT IN **DECLINES**

◓ =MED TRANSACTIONS COMPLETE WITH **MAJOR ERRORS**

○ =LOW TRANSACTIONS COMPLETE BUT WITH **MINOR ERRORS**;
FALLBACK/WORKAROUND IN PLACE

N/A **NO INFORMATION** AVAILABLE OR **NOT APPLICABLE**

2. Classification by Volume Impact

🔴 **HIGH NUMBER (BY PERCENTAGE OR ABSOLUTE VALUE)** OF DEVICES OR CARDS INVOLVED; BRAND IMPACT ---- EMV REPUTATIONAL IMPACT

◓ **POTENTIALLY HIGH** VOLUME; ROLLOUT CONTINUING;
PROBLEM FIX NOT DEFINED OR DELAYED

○ **LOW** VOLUMES; CONTROLLED PILOT; PROBLEM FIX IMPLEMENTED

N/A **NO INFORMATION** AVAILABLE OR **NOT APPLICABLE**

3. Classification of Field Implementation Status (NEW)

🔴 **NO PROGRESS (MAJOR DELAYS** OR **NO MOVEMENT AT ALL)**

◓ **SLOW PROGRESS (MINOR DELAYS** OR **UNDER MAINTENANCE MODE)**

○ **GOOD PROGRESS (REPLACEMENT ACTIVELY ONGOING)**

N/A **NO INFORMATION AVAILABLE** OR **NOT APPLICABLE**

***NOTES:**

Classification for #1 and #2 problem impacts and for #3 Field Implementation Status will be primarily based on information from the payment system. If no or limited data on problem impact is available from a payment system, the IWG will use its best judgment to properly classify it. Problems reported by the payment system will be rated high or medium based upon the rating assigned in the notification. The original rating will not be changed during the lifecycle of the issue so as to preserve the history of the initial impact, but changes in the status will be updated as "Current Assessment".

3 Details

3.1 Issues Summary

The table below and the sections following summarize the interoperability issues reported to the IWG. Actions resulting from these issues are either the responsibility of EMVCo or the payment system. In some cases, a particular issue may affect both EMVCo and the payment system for actions and/or resolution. Therefore, the issues have also been grouped by the "actors" who are primarily managing them -- EMVCo, Payment System, or Both. Since the last publication of this list, one issue has been closed with no new issues entering the List

	EMVCo	Both EMVCo and Payment System	Payment System	Total
Assessment in Process	0	0	0	**0**
Resolution in Process	0	0	0	**0**
Pending Implementation	0	0	0	**0**
Open Issues	0	0	0	**0**
Closed Issues	31 (I0062, I0050, I0048, I0047, I0045, I0043, I0041, I0038, I0036, I0031, I0030, I0029, I0027, I0026, I0025, I0024, I0023, I0022, I0021, I0016, I0015, I0013, I0012, I0011, I0010, I0007, I0006, I0005, I0004, I0002, I0001)	33 (I0091, I0090, I0089, I0088, I0087, I0086, I0085, I0084, I0083, I0082, I0081, I0080, I0079, I0078, I0077, I0076, I0075, I0074, I0073, I0069, I0068, I0065, I0064, I0061, I0060, I0057, I0058, I0055, I0054, I0051, I0049, I0046, I0044)	27 (I0072, I0071, I0070, I0067, I0066, I0063, I0059, I0056, I0053, I0052, I0042, I0040, I0039, I0037, I0035, I0034, I0033, I0032, I0028, I0020, I0019, I0018, I0017, I0014, I0009, I0008, I0003)	**91**
Total Issues	31	33	27	**91**

3.2 Assessment in Process – EMVCo

(none)

3.3 Assessment in Process -- EMVCo, Payment System

(none)

3.4 Assessment in Process -- Payment System

(none)

3.5 Resolution in Process -- EMVCo

(none)

3.6 Resolution in Process -- EMVCo, Payment System

(none)

3.7 Resolution in Process -- Payment System

(none)

3.8 Pending Implementation – EMVCo

(none)

3.9 Pending Implementation -- EMVCo, Payment System

(none)

3.10 Pending Implementation -- Payment System

(none)

3.11 Closed -- EMVCo Activities Complete

EMVCo Identifier	I0062	**Transaction Severity** ◓=MED
Issue Identifier	I0062	**Volume Severity** ◓=MED
Status	Closed – EMVCo	
Date Opened	July 07, 2006	
Description	It was reported that some terminals do not accept the card with zero value in ATR historical bytes, sometimes fall back to magnetic stripe transaction.	
Findings	It seems that the terminals reject some Belgian cards which contain zero value(s) on the ATR. The terminal may not support the zero value(s) for the historical bytes in the ATR.	
Terminal Information	Some Cybernet JADE terminals	
Corrective Action	The terminals have been replaced	
Preventative Action	Best Practice regarding this issue has been published on the website.	
Additional Comments		

EMVCo Identifier	I0050	**Transaction Severity** *N/A*
Issue Identifier	I0050	**Volume Severity** *N/A*
Status	Closed – EMVCo, Jan 25, 2004	
Date Opened	Dec 3, 2003	
Description	It was reported that EMV chip cards are not accepted at French chip-capable devices displaying the payment system logo. Only French bankcards are currently accepted.	
Findings	This is a similar issue to I0041 with the non-acceptance of ICC cards at devices with a payment system logo.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	Payment systems MasterCard and Visa are aware of the issue. These are not EMVCo-approved ICC devices. For EMVCo informational purposes only.	

EMVCo Identifier	I0048	**Transaction Severity** ●=HIGH
Issue Identifier	I0048	**Volume Severity** ◓=MED
Status	Closed – EMVCo, Jan 8, 2004	
Date Opened	Oct 01, 2003	
Description	It was identified that some cards had been personalized with Track 2 data and extra padding bytes. This caused authorization rejections by some Acquirers.	
Findings	When Track 2 equivalent data on the chip does not end on a full byte boundary, padding is required to bring the data element length to a full byte. Issuers personalized cards with extra padding bytes that caused rejection of the cards by some Acquirers.	
Corrective Action	Acquirer host software was modified to accept the cards. The cards will be corrected.	
Preventative Action	The CTWG published Application Note #18 in Dec, 2003, to clarify that the field shall be padded with a single hex ‘F’, if needed, to ensure whole bytes.	
Additional Comments	None.	

EMVCo Identifier	I0047	**Transaction Severity** ●=HIGH
Issue Identifier	I0047	**Volume Severity** ◓=MED
Status	Closed -- EMVCo, PS Oct 15, 2004	
Date Opened	Oct 01, 2003 – Sept 22, 2004	
Description	It was reported that the allowable padding of FF and 00 in the FCI data and within a record caused issues with personalization and interoperability.	
Findings	Some cards were personalized with additional padding that caused rejection of the cards at various terminals.	
Corrective Action	The error was identified and the personalization process corrected.	
Preventative Action	Application Note #22 was published in Sept 2004 to clarify the padding of constructed data objects. Here is a section from the application note: Padding, using ‘00’ or ‘FF’ bytes, may occur before, between or after primitive BER-TLV encoded data objects in the value field of constructed data objects (templates) only. This padding is subject to following rules: • 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 length byte of a padded constructed data object shall include any padding bytes present, since the padding shall only occur within the value field. The padding bytes have no meaning and are discarded.	
Additional Comments	None.	

EMVCo Identifier	I0045	**Transaction Severity** ●=HIGH
Issue Identifier	I0045	**Volume Severity** ○=LOW
Status	Closed – EMVCo, Feb 6, 2004	
Date Opened	Aug 01, 2003	
Description	It was reported that some terminals rejected cards where the Language Preference tag had been omitted in the PSE setting (FCI of the PSE) but the tag was present in the application’s ADF.	
Findings	Language preference, if used, needs to be identical in both the FCI of an ADF and the PSE. This was a card personalization issue. During application selection, the terminal checked the fields and rejected the card.	
Corrective Action	The cards were corrected and re-issued. The terminal is also being updated to not check for the discrepancy.	

Preventative Action	The CTWG published Specification Update #29 in June 2004, to clarify that terminals should not terminate the transaction when errors are found in the non-critical data elements during application selection.	
Additional Comments	None.	

EMVCo Identifier	I0043	**Transaction Severity** *N/A*
Issue Identifier	****	**Volume Severity** *N/A*
Status	Closed – EMVCo, Mar 13, 2003	
Date Opened	Feb 11, 2003	
Description	It was reported that ICC cards are rejected at chip capable devices. The device accepts only domestic brand cards.	
Findings	It was determined that although the device does not display an international payment system's logo, it is a chip capable device. These chip capable devices accept only the domestic brand.	
Corrective Action	None	
Preventative Action	None	
Additional Comments	For EMVCo informational purposes only. These are proprietary devices accepting the domestic ICC card. There is no payment system logo on these chip capable devices.	

EMVCo Identifier	I0041	**Transaction Severity** ●=HIGH
Issue Identifier	I0041	**Volume Severity** ◓=MED
Status	Closed – EMVCo, Jan 25, 2004	
Date Opened	Jul 10, 2002	
Description	It was reported that ICC cards are not accepted at chip capable devices that display the payment system (Visa or MasterCard) logos.	
Findings	It was determined that ICC cards are not accepted at various devices, including payphones and unattended petrol devices, where a payment logo is displayed. Proprietary ICC cards or magnetic stripe-only payment system cards are accepted. Payment system's ICC cards are rejected, and fallback to magnetic stripe does not occur.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	The payment systems MasterCard and Visa are aware of the issue. These are not EMVCo-approved ICC devices. Based upon the payment system logo on a terminal, there is currently no way to distinguish between magnetic stripe and chip card acceptance. For EMVCo informational purposes only.	

EMVCo Identifier	I0038	**Transaction Severity** *N/A*
Issue Identifier	I0038	**Volume Severity** *N/A*
Status	Closed –- EMVCo, Jan 21, 2003	
Date Opened	Dec 15, 2002	
Description	A request for technical clarification of the specifications was submitted concerning the proper use of Issuer script identifiers.	
Findings	The inquiry was responded to. No changes are needed.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0036	**Transaction Severity** ●=HIGH
Issue Identifier	I0036	**Volume Severity** ○=LOW
Status	Closed –- EMVCo, Mar 24, 2003	
Date Opened	Dec 15, 2002	
Description	It was reported that an interoperability issue could arise when cards configured to require cardholder confirmation during application selection are used at devices that do not support cardholder confirmation.	
Findings	The potential for this interoperability problem is known and is not in conflict with EMV specifications.	
Corrective Action	None.	
Preventative Action	Application Note #9, regarding the application priority indicator and cardholder confirmation, is now published to provide guidance to issuers on the coding of the card for cardholder confirmation.	
Additional Comments	This issue is related to issues I0010 & I0013.	

EMVCo Identifier	I0031	**Transaction Severity** *N/A*
Issue Identifier	****	**Volume Severity** *N/A*
Status	Closed –- EMVCo, Mar 18, 2003	
Date Opened	Oct 11, 2002	
Description	This was a technical question regarding the use of a particular field (TA4 in the ATR) and was not an interoperability issue.	
Findings	The inquiry was responded to. TA4 can be present provided that the rest of the ATR is correctly constructed.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	This is not an EMV issue. Queries of a technical nature can be submitted at the EMVCo website, under 'Communication'.	

EMVCo Identifier	I0030	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – EMVCo, May 21, 2004	
Date Opened	Oct 11, 2002	
Description	It was reported that a terminal application generated an error while attempting to process responses from a card. Both the card and the terminal used the same optional instruction for different purposes.	
Findings	It was determined that the terminal improperly handled the data received from the card. This error occurred when the terminal acted upon coincidental receipt of an inverse value of the instruction byte of the command. Receipt of this inverse value triggered the terminal to perform an invalid process.	
Corrective Action	The terminal application is being modified to correct the problem.	
Preventative Action	While this is a logic flaw unique to this terminal application, EMVCo test cases are being created to ensure this problem cannot occur again. Type Approval Level 1 test case updates were published in May, 2004. Lab implementations of the test cases will occur in several months.	
Additional Comments	None.	

EMVCo Identifier	I0029	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ◒=MED
Status	Closed – EMVCo Mar 14, 2003	
Date Opened	Oct 11, 2002	
Description	It was reported that a terminal application was rejecting a TLV value with a length of less than 127 bytes when represented by a 2-byte length.	
Findings	The terminal application is not functioning correctly as EMV requires that the aforementioned TLV lengths be supported.	
Corrective Action	The terminal application was modified to correct the problem.	
Preventative Action	Two additional test cases (2CE.001.01 & 2CE.001.02) were added in January 2003, to test for this particular condition.	
Additional Comments	None.	

EMVCo Identifier	I0027	**Transaction Severity** *N/A*
Issue Identifier	****	**Volume Severity** *N/A*
Status	Closed – EMVCo, Nov 22, 2002	
Date Opened	Oct 4, 2002	
Description	Interoperability problems were reported with a previously approved EMV device.	
Findings	It was determined that the approved device was subsequently modified to interface with a proprietary application. The reported errors apparently occurred only after that modification.	
Corrective Action	The modified application must be resubmitted for EMVCo approval.	
Preventative Action	None.	
Additional Comments	None.	

EMVCo Identifier	I0026	**Transaction Severity** *N/A*
Issue Identifier	****	**Volume Severity** *N/A*
Status	Closed -- EMVCo, Mar 31, 2003	
Date Opened	Oct 4, 2002	
Description	It was reported that a date handling error was encountered during testing of a terminal application.	
Findings	The date handling error was correctly identified during the testing of the terminal application. This problem was not encountered in a production environment.	
Corrective Action	None.	
Preventative Action	There is a test case for this condition. More information on the error was requested.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0025	**Transaction Severity** *N/A*
Issue Identifier	****	**Volume Severity** *N/A*
Status	Closed – EMVCo, Nov 22, 2002	
Date Opened	Oct 4, 2002	
Description	It was reported that a card was being rejected by a particular terminal application.	
Findings	It was determined that the failure occurred when processing a proprietary Tag. The processing of proprietary Tags is outside the scope of EMV.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0024	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – EMVCo, Jun 25, 2003	
Date Opened	Oct 4, 2002	
Description	It was reported that potential interoperability issues could arise in the future at particular ATM devices when offline PIN authentication is supported by both the card and device.	
Findings	This is a network and payment system issue that is not an EMV issue.	
Corrective Action	None.	
Preventative Action	Specification Update #16, 'If Cash or Cash back CVM Condition Codes', addresses this issue.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0023	**Transaction Severity** *N/A*
Issue Identifier	****	**Volume Severity** *N/A*
Status	Closed – EMVCo, July 1, 2003	
Date Opened	Oct 4, 2002	
Description	It was reported that multiple application cards were not being accepted by a certain terminal application.	
Findings	Additional information is needed concerning the card, terminal, and application types involved.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	The Type Approval Working Group requested additional information on the error. Since no additional information has been received, the issue was closed in July 2003.	

EMVCo Identifier	I0022	**Transaction Severity** *N/A*
Issue Identifier	****	**Volume Severity** *N/A*
Status	Closed – EMVCo, July 1, 2003	
Date Opened	Oct 4, 2002	
Description	It was reported that a card was rejected due to the presence of an invalid value in the Application Transaction Counter (ATC) field.	
Findings	This was a single, isolated occurrence and additional information is needed to research the issue further.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	The Type Approval Working Group requested more details on the error, especially if the card correctly sent the ATC. Since no additional information has been provided, the issue was closed in July 2003.	

EMVCo Identifier	I0021	**Transaction Severity** *N/A*
Issue Identifier	****	**Volume Severity** *N/A*
Status	Closed – EMVCo, July 1, 2003	
Date Opened	Oct 4, 2002	
Description	It was reported that sporadic SDA failures were being experienced.	
Findings	It was found that the rejected cards were subsequently processed successfully at other terminals. Additional information is necessary to research the issue further.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	The Type Approval Working Group requested more details on the error in order to make an assessment. Since no additional information was received, the issue was closed July 2003.	

EMVCo Identifier	I0016	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – EMVCo, Mar 31, 2003	
Date Opened	Oct 10, 2002	
Description	It was reported that a PIN Pad model was rejecting some cards.	
Findings	It was determined that the problem resulted from improper circuitry in the PIN Pad. The PIN Pad was rejecting cards as the result of testing for I/O at an EMV-defined indeterminate time.	
Corrective Action	Vendor has corrected the problem and the device received EMVCo approval.	
Preventative Action	None.	
Additional Comments	None.	

EMVCo Identifier	I0015	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ●=HIGH
Status	Closed – EMVCo, Mar 3, 2003	
Date Opened	Oct 4, 2002	
Description	It was reported that some cards were being rejected at particular ATM devices.	
Findings	It was determined that ATM devices were encountering an error selecting and processing an application on the card that was not EMV compliant. The proprietary application being selected relied upon use of a proprietary terminal application that is outside the scope of EMV.	
Corrective Action	The vendor has identified a solution and is developing the correction. Performing ISO 7816-4 SELECT per AID (equivalent to the EMV SELECT) of the application first would avoid this problem.	
Preventative Action	The Card Terminal Working Group has published a draft bulletin addressing non-EMV cards and the application selection methodology after the answer to reset.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0013	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – EMVCo, Oct 10, 2002	
Date Opened	Jan 14, 2002	
Description	It was reported that a terminal application rejected cards requiring cardholder confirmation.	
Findings	It was determined that the cards being rejected were configured to require cardholder confirmation for application selection, however, the terminal application did not support cardholder confirmation. According to EMV, this is the correct terminal behavior.	
Corrective Action	The Acquirer will modify the terminal parameters to correct the incompatibility.	
Preventative Action	Application Note #9 was published March 2003, to provide guidance to issuers on the coding of the card for cardholder confirmation.	
Additional Comments	This is the same issue as I0010 and I0036.	

EMVCo Identifier	I0012	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ◓=MED
Status	Closed – EMVCo, Oct 10, 2002	
Date Opened	Jan 14, 2002	
Description	It was reported that some cards were "locking-up" particular terminal applications.	
Findings	It was determined that terminal applications were rejecting cards with a Language Preference containing uppercase letters. This data field should have been encoded with lower case letters.	
Corrective Action	This is a personalization issue with the card.	

Preventative Action	EMVCo Application Note #12 was published July 2003, to clarify the coding of upper and lower case. ISO 639 indicates the usage of lower case, so cards shall use lower case for language preference. However, it is highly recommended that terminals not be case-sensitive and recognize the language preference regardless of its case.
Additional Comments	None

EMVCo Identifier	I0011	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – EMVCo, Nov 22, 2002	
Date Opened	Jan 14, 2002	
Description	It was reported that some cards were causing a terminal application to generate an “Invalid Data” response.	
Findings	It was determined that the terminal application was improperly rejecting cards when either an Application Label or Application Preferred Name field contained a ‘space’ character. The EMV specifications state that these fields may only contain alphanumeric characters and was interpreted by the terminal vendor to mean the exclusion of special characters such as ‘space’.	
Corrective Action	The terminal application was modified to additionally accept special (printable) characters.	
Preventative Action	EMVCo Specifications Update Bulletin #14 is now published on the website.	
Additional Comments	None.	

EMVCo Identifier	I0010	**Transaction Severity** N/A
Issue Identifier	****	**Volume Severity** N/A
Status	Closed – EMVCo, Nov 22, 2003	
Date Opened	Aug 27, 2002	
Description	It was reported that a terminal application was incorrectly rejecting cards requiring cardholder confirmation.	
Findings	It was determined that the cards being rejected were configured to require cardholder confirmation for application selection; however, the terminal application did not support cardholder confirmation. According to EMV, this is the correct terminal behavior.	
Corrective Action	The Acquirer will modify the terminal parameters to correct the incompatibility.	
Preventative Action	Application Note #9 was published March, 2003, to provide guidance to issuers on the coding of the card for cardholder confirmation.	
Additional Comments	None.	

EMCo Identifier	I0007	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ◓=MED
Status	Closed – EMVCo, Jun 20, 2003	
Date Opened	Aug 27, 2002 & Oct 4, 2002	
Description	It was reported that T=1 cards configured with TA2 in the Answer to Reset (ATR) are being rejected by a terminal application.	
Findings	The EMV3.1.1 and EMV4.0 specifications (Book 1, section 4.3.3.5) and test cases 1CE.005.xy and 1CE.006.xy have been reviewed. The specifications and the test cases are correct. An ATR with a TA2 is accepted provided that b5=0 and other conditions are satisfied.	
Corrective Action	None	
Preventative Action	None	
Additional Comments	Please check to see if this is an approved EMVCo device.	

EMVCo Identifier	I0006	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – EMVCo, Sep 9, 2003	
Date Opened	Aug 27, 2002 and Oct 10, 2002	
Description	It was reported that a terminal application was rejecting T=1 cards configured with TC1=FF in the Answer to Reset.	
Findings	A card with the error was received from the Issuer. The TAWG reviewed the issue. Current tests do not test for the maximum INF field. A modified test using an I-Blocks with a maximum INF field size (254 bytes) shall be implemented by the TAWG in the accredited laboratories. This test case implementation will be used in Type Approval at each EMVCo accredited laboratory.	
Corrective Action	The test case has been modified.	
Preventative Action	The TAWG has additionally reviewed the approved labs' test case implementations.	
Additional Comments	None.	

EMVCo Identifier	I0005	**Transaction Severity** ◓=MED
Issue Identifier	*****	**Volume Severity** ◓=MED
Status	Closed – EMVCo, May 21, 2004	
Date Opened	Oct 10, 2002	
Description	It was reported that a terminal application was improperly interpreting the first 2-bits of the CVM Results as '00'.	
Findings	This condition was confirmed and is in violation of EMV.	
Corrective Action	Test case 2CM.028 will be enhanced to test for this specific occurrence.	
Preventative Action	Further clarification was added in the Level 2 test plan improvements, published May 2004. Lab implementations of the test cases will occur in the next few months.	
Additional Comments	None.	

EMVCo Identifier	I0004	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – EMVCo, Mar 31, 2003	
Date Opened	Aug 27, 2002 & Oct 4, 2002	
Description	It was reported that a terminal application incorrectly accepted a response to a GENERATE AC command that contained an invalid length and continued processing the transaction request.	
Findings	Two test cases exist, 2CL.034 and 2CA.011, to test for the Generate AC and the DDOL. This issue is an earlier (older) problem that is today corrected in the various implementations of the EMVCo test cases.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	Please check to see that the terminal is an approved device.	

EMVCo Identifier	I0002	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – EMVCo, Mar 31, 2003	
Date Opened	Oct 4, 2002	
Description	It was reported that a terminal application rejected the ICC card when the FCI template of the card was padded with zeros.	
Findings	EMV specifies that the terminal application should ignore the padding of zeros in the FCI template. EMV test 2CL.052.00 tests for zero padding.	
Corrective Action	The terminal application was modified to correct the error.	
Preventative Action	Type Approval test case updates were published in May, 2004. Lab implementations of the test cases will occur in the next few months.	
Additional Comments	None.	

EMVCo Identifier	I0001	**Transaction Severity** ◒=MED
Issue Identifier	****	**Volume Severity** *N/A*
Status	Closed – EMVCo, Jan 22, 2003	
Date Opened	Aug 27, 2002	
Description	It was reported that a terminal application was incorrectly recording an error in the Terminal Verification Results (TVR) field when a DDA failure occurred as the result of a missing ICC Public Key Remainder in the consumer card. When this error occurred, the terminal application was setting only the TVR bit corresponding to ‘ICC Data Missing’ and no other bits – such as ‘Offline dynamic data authentication failed’.	
Findings	EMV specifies that the terminal application need only set the TVR bit corresponding to ‘ICC Data Missing’ as is presently occurring. Attempting to perform DDA would not be possible with the absence of the ICC Public Key Remainder.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	None.	

3.12 Closed -- EMVCo, Payment System Activities Complete

EMVCo Identifier	**I0091**	**Tag5F20 Chinese character encoding issue**
Date	Opened - Jun 4, 2014	Closed - Aug 22, 2017
Original Assessment	**Transaction Severity** ● =HIGH	**Volume Severity** ◓ =MED
Current Assessment	**Transaction Severity** ● =HIGH	**Volume Severity** ○ =LOW
Current Status	Pending Implementation – EMVCo, Payment System	**Field Implementation** ○ =GOOD
Description	Some cards in the field contain Chinese characters in Tag5F20 which cannot be accepted on some terminals (currently only ATM, still checking POS) in Europe. The terminal is expecting ASCII in this tag but Issuer use GBK character set (a Chinese national standard for encoding Chinese characters). Other tags could have similar issue are tag50, tag9F0B, tag9F1F, tag9F12, tag5F50.	
Findings	Transactions on such cards will be rejected by some terminals which check the format of these tags. The incident has been reported in France and UK	
Terminal Information	Wincor ATMs	
Corrective Action	Wincor has new kernels based on 4.3b available to update impacted ATMs. ATMs have been updated and no further incidents reported.	
Preventative Action	Issued Spec Bulletin No159 in Feb 2015 which updates Spec Bulletin No83 issued in Dec 2010. The terminals now must ignore the formatting error and continue processing for Tags 5F20, 9F0B, 5F50, 9F4D, and 9F4F. Added relevant test cases to 4.3d in May 2015 (TA Bulletin No160)	
Additional Comments	CLOSED. No new field issues reported in the last 12 months with all necessary preventative actions taken.	

EMVCo Identifier	**I0090**	**Terminal unable to process cards with longer length AFLs and causes online crypto to fail**
Date	Opened - Feb 20, 2012	Closed – Aug 7, 2013
Original Assessment	**Transaction Severity** ◓ =HIGH	**Volume Severity** ○ =LOW
Current Assessment	**Transaction Severity** ◓ =HIGH	**Volume Severity** ○ =LOW
Current Status	Resolution in Process – EMVCo, Payment System	**Field Implementation** ○ =GOOD
Description	It was reported that certain transactions are being declined due to online crypto validation error in the authorization message. The issue has been identified in transactions initiated by some terminals in Taiwan.	

Findings	The cause of the issue is likely to be that the terminal is unable to correctly process cards that have longer length Application File Locator (AFL). Although the terminal to card portion of the transaction appears to complete without problems, the Application Interchange Profile (AIP) that is sent in the online authorization is overlaid with two bytes from the end of the AFL. This incorrect AIP causes the online cryptogram (ARQC) to fail validation and the transaction to be declined.
Terminal Information	VeriFone 3750 and 5150 terminals
Corrective Action	Fixed kernels being downloaded or being swapped out with new terminals.
Preventative Action	Test Plan 4.2a –introduced after this kernel approval- added a test for longer AFLs (150 bytes). This tested length seems sufficient. As a consequence EMVCo does not foresee additional test unless the on-going investigation leads to a different understanding of the issue.
Additional Comments	CLOSED. The impacted terminals have either aged out of the market or have received updated applications/kernels that do not exhibit the issue. No issues reported for over 12 months

EMVCo Identifier	**I0089**	**Issue with padding bytes at end of PSE read response**
Date	Opened - May 23, 2011	Closed – Mar 17, 2016
Original Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ◓=MED
Current Status	Resolution in Process – EMVCo, Payment System	**Field Implementation** ○=GOOD
Description	In a range of VeriFone terminals, the transaction hangs during application selection for certain German issued cards with padding bytes at the end of a PSE read record response after the constructed data object 0x61. No transaction available (chip or mag stripe) when issue occurs.	
Findings	The impacted kernels get into an endless loop when reading the PSE Read record response because they does not skip the '0' padding bytes in the PSE read response. Issue initially reported in Netherlands, Luxembourg, Poland and Australia. Other countries identified after the assessment especially in Asia and Canada.	
Terminal Information	Several VeriFone kernels including Vx EMV Module 5.0.5, Vx EMV Module 5.1.5, SC5000 EMV Module 4.5.0.	
Corrective Action	Corrected versions have been made available for all impacted kernels. EMVCo lists "Level 2 Contact Approved Application Kernels" and "Level 2 Contact Approved Application Kernels - Restricted Renewal" have been updated removing impacted kernels and appended references of corrected versions. Upgrade globally completed in all countries with maybe some restriction for Canada.	
Preventative Action	Additional test cases added to terminal testing process (4.3.a).	

Additional Comments	CLOSED - No new field issues reported in the last 12 months with all necessary preventative actions taken.

EMVCo Identifier	**I0088**	**Contactless reader issues during mobile transactions**
Date	Opened - Apr 13, 2011	Closed – Sep 13, 2016
Original Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ○=LOW
Current Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ○=LOW
Current Status	Resolution in Process – EMVCo, Payment System	**Field Implementation** ○=GOOD
Description	The contactless reader exhibits non-standard behavior when it is conducting a payment transaction with a GSM mobile phone if the mobile receives a call. This non-standard behavior involves the initiation of a power-up reset. The reader remains in reset until the phone stops transmitting. Recovery can require re-booting of the reader. In some case, the incident causes a permanent reversal of the reader's display screen (i.e. a mirror image displays).	
Findings	The cardholder device is a mobile device using GSM850 and GSM 900 frequency band. The incident has been reported in the UK	
Terminal Information	VivoPay 5000	
Corrective Action	A hardware fix has been developed that solves the problem.	
Preventative Action	EMD Task Force defined the methodology to investigate for future EMD issues.	
Additional Comments	No issues in the field. Investigation methodology defined. Re-assess further necessity of preventative measures based on future related issues should they arise.	

EMVCo Identifier	**I0087**	**Terminal error due to use of private tags**
Date	Opened - Dec 21, 2010	Closed – Mar 17, 2016
Original Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Status	Pending Implementation – EMVCo, Payment System	**Field Implementation** ◓=SLOW **Under Maintenance Mode*
Description	In certain VeriFone kernels, during Application selection, when the kernel tries to update the Tag DF10 (private tag) read from the card's response to the collection, it returns an error.	
Findings	Tag DF10 is used by the kernel internally for other usage. Some UK issued cards were affected as the terminal terminates the transaction due to the duplicate usage of tag DF10.	
Terminal Information	VeriFone Vx EMV Module 5.0.0 affected.	
Corrective Action	VeriFone has developed a patch fix which has passed relevant testing, and is now on the EMVCo website.	
Preventative Action	Additional test cases added to terminal testing process 2CJ.012.04 in 4.3	

Additional Comments	CLOSED - No new field issues reported in the last 12 months with all necessary preventative actions taken.

3

EMVCo Identifier	**I0086**	**Terminal not following signal sequence during warm reset**
Date	Opened - Apr 23, 2010	Closed – March 28, 2016
Original Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Status	Resolution in Process – EMVCo, Payment System	**Field Implementation** ○=GOOD
Description	It was reported that certain terminals deactivate the Clock signal by setting CLK at state L during the warm reset sequence. Such a sequence is identified by silicon manufacturer(s) as a potential threat requiring the implementation of a counter measure. In some cases this may lead to disabling the card. The transaction is not possible and the card may be damaged or disabled by internal security mechanism.	
Findings	The terminal's behavior seems not compliant to EMV v.4.1 and v.4.2 Book 1 section "6.1.3.2 Warm Reset" Details still under investigation.	
Terminal Information	Not relevant. This defect was introduced by third parties' development specific to few markets and not by the terminals vendor (as per EMVCo definition)	
Corrective Action	A fix on the application layer made available.	
Preventative Action	New test added through the introduction of a new test tool hardware. (EMVCo Contact Terminal L1 Test Case 1CC.004.0x with Comprion IT3).	
Additional Comments	CLOSED. Corrective and preventative actions completed. No new incidents reported in over 12 months.	

EMVCo Identifier	**I0085**	**Terminal freeze due to Certificate serial number issue**
Date	Opened - Feb 25, 2010	Closed – Jan 18, 2011
Original Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Status	Pending Implementation – EMVCo, Payment System	**Field Implementation** ◓=SLOW **Under Maintenance Mode*
Description	It was reported that certain VeriFone terminals are unable to process certain cards with long key length and supporting Offline Enciphered PIN and when the cards are used in a certain sequence. This issue happens when the first bytes of Issuer Certificate serial numbers of two consecutive cards differ by a small number. If two such cards are used then the first transaction succeeds but the next one freezes the terminal. All that matters is the difference between Issuer Certificate serial numbers of the two cards.	
Findings	The issue has only been reported in the UK.	
Terminal Information	VeriFone Vx 3.0.5 terminals	
Corrective Action	The vendor has developed a fix for this issue to be used in the interim prior to ultimately updating to a new EMVCo approved	

	kernel. It was confirmed that the fix successfully solved the issue with no critical errors in regression testing This kernel did not go through Renewal Testing as per EMVCo process, therefore it remains not formally EMVCo approved. Still the patch provides an effective solution to a critical existing issue, thus the deployment of this corrected version should be considered by the acquirers. Prior to field deployment, Acquirers are required to consult with the relevant Payment Systems.
Preventative Action	This is an incident that can happen in very specific scenarios and no specific test cases could be defined.
Additional Comments	CLOSED due to no issues being reported over 10 months with limited (low) terminals/cards affected.

EMVCo Identifier	**I0084**	**ESD issue with Dual Interface Cards**
Date	Opened – Mar 16, 2010	Closed – Mar 17, 2016
Original Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ●=HIGH
Current Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ◓=MED
Current Status	Resolution in Process – EMVCo, Payment System	**Field Implementation** ◓=SLOW **Under Maintenance Mode*
Description	It was reported that certain contact chip PIN pads in Canada sometimes experience ESD issues when reading dual interface cards via the contact chip interface. In most cases the terminal automatically recovers. In some cases if the device is integrated with a merchant till, the till needs to be reset. With repeated discharges, the device may not recover or become non-functional.	
Findings	It was confirmed that dual interface cards are not the only card types impacted.	
Card/Terminal Information	VeriFone Vx810 terminals in Canada were found to be particularly susceptible to ESD, but field modification has already been made available.	
Corrective Action	This problem occurs in cold, dry environments. Canadian acquirers decided to replace affected terminals with different model of terminals. VeriFone has provided field modification solutions with most problematic ones replaced and others replaced in maintenance cycle.	
Preventative Action	A dedicated task force within EMVCo was created to address this issue. Terminal ESD Evaluation Process released in Sep 2014.	
Additional Comments	CLOSED - No new field issues reported in the last 12 months with all necessary preventative actions taken.	

EMVCo Identifier	**I0083**	**"PIN entry required and PIN pad not present or not working" bit set while Offline PIN is not supported by the terminal**
Date	Opened - Jan 20, 2010	Closed – Jul 27, 2011

Original Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Status	Pending Implementation – EMVCo, Payment System	**Field Implementation** ◓=SLOW **Under Maintenance Mode*
Description	It was reported that a significant number of cards were declined offline when used in certain terminals in Hong Kong. Apparently, the terminals try to conduct the PIN-related CVM processing even when the terminal doesn't support any PIN-related CVMs and the CVM condition code of the cards indicates "if supported" result in set the "PIN entry required and PIN pad not present or not working" bit of the TVR to 1 regardless of the value of the CVM condition code.	
Findings	The issue was also reported in China, Macau, Singapore, and Vietnam.	
Card/Terminal Information	PAX P60 and P70 terminals	
Corrective Action	In progress through terminal replacement. Hong Kong, China, and Macau – 80% complete Singapore and Vietnam – Unknown, but no actual issues reported	
Preventative Action	The new test case has been introduced in the 4.2.b test case, effective from end of January 2010.	
Additional Comments	CLOSED - No new field issues reported in the last 12 months with all necessary preventative actions taken.	

EMVCo Identifier	**I0082**	**Transaction declined when Issuer Authentication fails**
Date	Opened - Dec 21, 2009	Closed – Mar 17, 2016
Original Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Status	Pending Implementation – EMVCo, Payment System	**Field Implementation** ◓=SLOW
Description	It was reported that some IBM ATMs in Canada decline issuer-approved transactions when issuer authentication fails even though the card returns an approval (TC) in the second GEN AC response. This behavior violates the EMV specification and causes a decline for transactions that should be approved. Issuer has personalized cards to not decline when Issuer Authentication fails and the issuer has approved the transaction online, but the ATM in Canada is declining regardless.	
Findings	ATM declines issuer-approved transactions when Issuer Authentication fails even though card approves transactions. Error occurs when EXTERNAL AUTHENTICATE command is used for Issuer Authentication.	
Terminal Information	The ATM hardware is supplied by IBM, and the ATM software is written by Wincor Nixdorf.	
Corrective Action	The client is running Wincor Nixdorf software on ATMs managed by IBM. The fix has been completed and tested by Wincor	

	Nixdorf. The fix will be implemented as part of the OS migration to Windows 7.
Preventative Action	The new test case has been introduced in the 4.2.b test case, effective from end of January 2010.
Additional Comments	CLOSED - No new field issues reported in the last 12 months with all necessary preventative actions taken.

EMVCo Identifier	**I0081**	**Clock Instability in terminal causes cards to shutdown**
Date	Opened - Dec 21, 2009	Closed - Mar 28, 2016
Original Assessment	**Transaction Severity** ○=LOW	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ○=LOW	**Volume Severity** ○=LOW
Current Status	Pending Implementation – EMVCo, Payment System	**Field Implementation** ○=GOOD
Description	It was reported that Ingenico I6400 terminals have a problem with its clock signal, which is perceived by some newer cards as a 'power glitch' attack so the card shuts down. Older cards are less sensitive and do not have this issue. After shut down, transaction is completed using magnetic stripe.	
Findings	Issue seems to be limited to approximately 5,800 Ingenico I6400MHQ001B approved terminals produced before July 2005. Some but not all of these devices have a problem with several card products. It was confirmed that this issue was identified in Norway.	
Terminal Information	Ingenico I6400	
Corrective Action	Replacement of the terminals completed.	
Preventative Action	New contact L1 test tool has been introduced which added glitch testing.	
Additional Comments	CLOSED. No new incidents have been reported in over 12 months.	

EMVCo Identifier	**I0080**	**Interference GSM/CDMA Dual Interface card**
Date	Opened - Jan 20, 2010	Closed – Jul 27, 2011
Original Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ○=LOW
Current Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ○=LOW
Current Status	Resolution in Process – EMVCo, Payment System	**Field Implementation** ◓=SLOW **Under Maintenance Mode*
Description	It was reported that there was an interference issue between several GPRS/GSM terminals and some chips used on Dual Interface cards.	
Findings	The technical issue is thought to be due to the emission of EMC by the terminal during the contact payment transaction which is interrupted at the card level (chip reset) during the online authorization communication and can not be completed even though the issuer returns the approval response. The issue is not systematic and will depend on factors influencing the transmission quality like the distance from the mobile operator transmitter. Very few incidents have been reported so far from the field and the current impact is maybe limited but there is a risk as deployment of terminals using wireless technology seems at its beginning.	

Card/Terminal Information	N/A
Corrective Action	Both the smartcard silicon manufacturer and the terminal vendor reported to have experienced field issues have enhanced their device designs to reduce the risk of such interference.
Preventative Action	Best Practices for Issuance and Acceptance of Dual Interface Cards published on the EMVCo website. A dedicated task force within EMVCo was created to address this issue. The current plan is to define risk inventory of radiation, conduct assessment and to define measurement methodology based on the above assessment.
Additional Comments	CLOSED - No new field issues reported in the last 12 months. Preventative measures for Electro Magnetic Disturbance/ Compatibility being addressed by dedicated task force.

EMVCo Identifier	**I0079**	**Transaction terminated when CDA cards used and CDA failed**
Date	Opened - Jan 26, 2009	Closed Nov 24, 2009
Original Assessment	**Transaction Severity** ◒=MED	**Volume Severity** ◒=MED
Current Assessment	**Transaction Severity** ◒=MED	**Volume Severity** ◒=LOW
Current Status	Pending Implementation – EMVCo, Payment System	**Field Implementation** ○=GOOD
Description	Certain terminals have a problem to process CDA failure transactions. The terminals don't allow transactions to go online for approval for cards that fail CDA.	
Findings	In case the terminal fails in recovering the RSA keys needed during the CDA process, the transaction is terminated even if the card responds with ARQC (go online) or TC (approve offline) in response to generate AC command. There is no issue if the card responds GENAC in format 1.	
Terminal Information	Verifone Vx/Verix and SC 5000 4.0.0 modules	
Corrective Action	Verifone has developed a Hot Fix for this issue and the recertification test was completed. The terminal upgrade has started.	
Preventative Action	It was confirmed that the most current test case checks that the terminal can correctly process a CDA failure transaction.	
Additional Comments		

EMVCo Identifier	**I0078**	**Card contact interface shuts down when contactless field is detected**
Date	Opened - Jan 26, 2009	Closed – Jul 27, 2011
Original Assessment	**Transaction Severity** ◒=MED	**Volume Severity** ○=LOW
Current Assessment	**Transaction Severity** ◒=MED	**Volume Severity** ○=LOW
Current Status	Resolution in Process – EMVCo, Payment System	**Field Implementation** N/A
Description	Some dual-interface cards shut down the contact interface when the card detects a contactless field. The presence of a stable RF	

	field is sufficient to cause this problem, as it is the energy of the field that powers the card's contactless interface and causes the issue. With some placements of the contact and contactless readers, a contact read of the card is not possible since the contactless interface is always detected while the card is being inserted into the contact reader. Note that the distance of the card from the contactless reader may be such that contactless communications are not sufficiently stable to conduct a transaction, but within range for the RF field to activate the cards contactless interface.
Findings	The card may also activate the contactless interface and disable the contact interface if there is an RF field originating from an unknown source, external to the payment acceptance environment. Issuers are impacted if the placement of the readers prevents a contact read and card settings require a contact read to update card-based data elements. Issuers issuing contact-only product on dual-interface cards with this issue may also be impacted. Merchants with contact and contactless acceptance may not be able to accept contact chip transactions if the card has this issue.
Card/Terminal Information	This was discovered through testing at labs, field issues have not been identified.
Corrective Action	N/A (no actual field issues)
Preventative Action	Best Practices for Issuance and Acceptance of Dual Interface Cards published on the EMVCo website. A dedicated task force within EMVCo was created to address this issue. The current plan is to define risk inventory of radiation, conduct assessment and to define measurement methodology based on the above assessment.
Additional Comments	CLOSED - No actual field issues reported and preventative measures for Electro Magnetic Disturbance/Compatibility being addressed by dedicated task force.

EMVCo Identifier	**I0077**	**ICC Public Key >= 1024 bit in Format 1 and Format 2**
Date	Opened - Nov 11, 2008	Closed - July 20, 2010
Original Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ●=HIGH
Current Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Status	Pending Implementation – EMVCo, Payment System	**Field Implementation** ○=GOOD
Description	Certain terminals in the field are wrongly failing DDA when the DDA card's ICC Public Key is greater than or equal to 1024 bits.	
Findings	There is a problem with certain DDA-supported terminals when a card's ICC Public Key is greater than or equal to 1024 bits. When the card responds to the INTERNAL AUTHENTICATE command using Format 1 and Format 2 templates, DDA supported terminals fail DDA. This issue occurs because the length field of the	

	INTERNAL AUTHENTICATE response is two bytes long when the key is 1024 bits or more.
Terminal Information	<DDA Issue> Ingenico TT41
Corrective Action	Ingenico has developed a Hot Fix for this issue and the recertification test was completed. 90% of the terminals will be upgraded, the remaining 10% of the terminals will be replaced. At the end of April 2010, download to the terminals in the field countries is progressing with 95% complete. Replacement of the terminals is progressing with 25% completete.
Preventative Action	It was confirmed that the most current test case checks that the terminal can process cards having ICC Public Key of 128 bytes and more.
Additional Comments	Majority of terminals are fixed, with the rest in maintenance mode replacement – this issue is closed.

EMVCo Identifier	**I0076**	**DDA fails with certain formats of ICC Dynamic Data**
Date	Opened - Nov 14, 2008	Closed - July 20, 2010
Original Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Status	Pending Implementation – EMVCo, Payment System	**Field Implementation** ◓=SLOW
Description	It was reported that Hypercom terminals are unable to process certain formats of ICC Dynamic Data. ICC Dynamic Data consists of an ICC Dynamic Data length byte, an ICC Dynamic Number length byte, a 2-8 byte ICC Dynamic Number, and optionally additional dynamic data.	
Findings	Most cards do not use the additional dynamic data, but certain Swiss cards use ICC Dynamic Data with this optional data. All Hypercom terminals fail DDA when they encounter this additional data.	
Terminal Information	Hypercom	
Corrective Action	11,000 terminals in Switzerland are known to be impacted. 9,000 have been upgraded with rest to be updated by February 2009.	
Preventative Action	Preventative test cases has been introduced by updating test plan ver. 4.2.a.	
Additional Comments	The issue in Switzerland has been corrected, no further issues reported in over 12months – closed.	

EMVCo Identifier	**I0075**	**Application Preferred Name with extended character**
Date	Opened - Sep 9, 2008	Closed – Sep 18, 2012
Original Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ○=LOW
Current Status	Resolution in Process – EMVCo, Payment System	**Field Implementation** N/A
Description	It was reported that certain Ingenico terminals have a problem to accept Turkish cards having an ï in the application preferred	

	name. This issue only happens in old Unicapt 16 Ingenico terminals in France.
Findings	This issue only happens in old Unicapt 16 Ingenico terminals in France.
Terminal Information	Ingenico Unicapt 16
Corrective Action	Ingenico has developed a Hot Fix for this issue and awaiting recertification.
Preventative Action	It was confirmed that the most current test case checks that the terminal can process cards having extended characters in the application preferred name.
Additional Comments	Closed: Most Unicapt 16 terminals have been replaced in France, and there have not been any new reports of this incident in over 2 years.

EMVCo Identifier	**I0074**	**Offline PIN Encryption Max Key Length**
Date	Opened - Sep 9, 2008	Closed – Sep 18, 2012
Original Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ○=LOW
Current Status	Resolution in Process – EMVCo, Payment System	**Field Implementation** N/A
Description	It was reported that certain Ingenico terminals have a problem to accept cards having ICC PIN Encipherment key of 128 bytes and more even if not used (CVM List without encrypted PIN).	
Findings	This issue only happens in old Unicapt 16 Ingenico terminals in France.	
Terminal Information	Ingenico Unicapt 16	
Corrective Action	Ingenico has developed a Hot Fix for this and awaiting recertification.	
Preventative Action	It was confirmed that the most current test case checks that the terminal can process cards having ICC PIN Encipherment key of 128 bytes and more.	
Additional Comments	Closed: Most Unicapt 16 terminals have been replaced in France, and there have not been any new reports of this incident in over 2 years.	

EMVCo Identifier	**I0073**	**Error with certain proprietary data**
Date	Opened - Aug 18, 2008	Closed - Jan 20, 2010
Original Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ◓=MED
Current Status	Pending Implementation – EMVCo, Payment System	**Field Implementation** ○=GOOD
Description	It was reported that certain Verifone terminals are unable to read SFIs 21-30 where issuer proprietary data is personalized and instead terminate the transaction when the read is attempted. It is still under investigation the same problem occurs when reading from SFIs 11-20 where payment system proprietary data is personalized.	

Findings	Cards that are personalized with an AFL requiring this data to be read are not accepted at the impacted terminals. There are about 205,000 impacted terminals in Brazil. Some Austrian ATMs also had this problem, but that problem has been corrected.
Terminal Information	Verifone Omni 3750 Verix 510
Corrective Action	Verifone has a corrected kernel available. 95,000 terminals have already been replaced, and the rest have also been replaced at the end of 2009
Preventative Action	It was confirmed that new test cases have been added to Test Plan 4.2.a which has been effective since end of Feb 2009.
Additional Comments	Problematic kernels have already been removed from the EMVCo Approval List and replaced with the fixed kernels where appropriate.

EMVCo Identifier	**I0069**	**Lock-up with certain PDOL data**
Date	Opened - Sep 18, 2006	Closed – June 24, ‘08
Original Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ○=LOW	**Volume Severity** ○=LOW
Current Status	Assessment in Process – EMVCo, Payment System	**Field Implementation** ○=GOOD
Description	When the card’s PDOL contains the tag for “Amount, Other” (tag 9F03) and in less frequent cases, the tag for “Amount, Authorized” (tag 9F02), the terminal displays ‘Invalid card’ and does not continue with the transaction.	
Findings	The transaction is unable to complete because the terminal locks up after application selection when these tags are encountered in the card’s PDOL. The problem does not occur at all devices with the impacted kernel but only in implementations with certain non-kernel software. The problem appears to be related to the interaction between the kernel and non-kernel software. Field research conducted so far have identified old terminals in UK and Taiwan as potentially affected markets.	
Terminal Information	Ingenico and Gemalto terminals	
Corrective Action	A workaround fix has been developed by the vendors and implemented onto the affected terminals. There have been no new reports on this issue. In light of the above, this issue is considered closed.	
Preventative Action	New test cases were introduced in the latest test plan (v.4.1.d) effective end of October 2007.	
Additional Comments	This problem has not been reported for any ‘live’ transactions. No current cards (to our knowledge) include these tags in their PDOLs, but it should be noticed that CPA cards with low-value profiles may use these tags in the future.	

EMVCo Identifier	**I0068**	**TLV data with ‘00’ length Issue**
Date	Opened - Oct 12, 2006	Closed – Feb 03, 2009
Original Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ○=LOW	**Volume Severity** ○=LOW

Current Status	Resolution in Process – EMVCo, Payment System	**Field Implementation** ◓=SLOW
Description	It has been reported that cards have been offline declined on two different POS acquired by the same UK acquirer. The transactions are finally accepted via manual PAN entry.	
Findings	Tests were conducted in the lab and it showed that the terminal stops the transaction during the READ RECORD command exchanges when receiving from the card a TLV data with L = "00" and V is not present (Data element 9F48 ICC Public Key Remainder). _A test case exists (TC 2CA.001.04) for the 4.0 and 4.1 EMV Spec version, but does not use this specific data for testing.	
Terminal Information	Trintech and Verifone	
Corrective Action	Trintech: Replacement completed. Verifone: New terminal has been developed. Replacement has not yet started.	
Preventative Action	New test cases were introduced in the latest test plan (v.4.1.d) effective end of October 2007.	
Additional Comments		

EMVCo Identifier	**I0067**	**Length limitation to the input for Hash**
Date	Opened - Oct 11, 2006	Closed – Jul 27, 2011
Original Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Status	Pending Implementation – Payment System	**Field Implementation** ◓=SLOW **Under Maintenance Mode*
Description	It was reported that some terminals which have a length limitation to the input of Hash for Offline Data Authentication certificates.	
Findings	The terminal is unable to compute the hash during the Offline CAM (SDA, DDA or CDA) if 150 or more bytes are signed (“Static Data to be Authenticated” as defined in EMV Book 2). Then the Offline CAM fails and potentially the cardholder verification if using Offline Encrypted PIN. This issue has been identified with terminals in UAE, Belgium, Brazil, Malaysia, New Zealand, Taiwan, and Hong Kong. Only one known issuer with such personalization parameter,	
Terminal Information	Verifone, Thales Artema	
Corrective Action	Verifone –Replacements ongoing in maintenance mode.. Thales – Replacement in UK has been completed. There are no issuers now using this personalization parameter.	
Preventative Action	Best Practice regarding this issue has been published on the website. Preventative test case has been included in Test Plan version 4.1.e effective as of May 2008.	
Additional Comments	CLOSED due to no issues being reported over 12 months with limited (low) terminals/cards affected.	

EMVCo Identifier	**I0065**	**Transaction Severity** ◓=MED
Issue Identifier	I0065	**Volume Severity** ◓=MED
Status	Closed – EMVCo, Oct 24, 2006	

Date Opened	July 07, 2006	
Description	It was reported that some terminals in Hungary continue to send the issuer script received at the former transaction to other issuer cards.	
Findings	It seems that the terminal continues to send the issuer script commands received in the previous transaction to the cards used in the next transaction without any reason.	
Terminal Information	Hypercom ICE 5500 in Hungary	
Corrective Action	Acquirer confirmed that the affected terminals have been replaced.	
Preventative Action	Preventative test case will be included in the next Test Plan version 4.1.c effective in January 2007.	
Additional Comments	None	

EMVCo Identifier	**I0064**	**Transaction Severity** ●=HIGH
Issue Identifier	I0064	**Volume Severity** ◓=MED
Status	Closed – EMVCo, Oct 24, 2006	
Date Opened	July 07, 2006	
Description	It was reported that some terminals do not manage the IAD (Issuer Authentication Data) correctly if the length is longer than 10 bytes.	
Findings	It seems that several transactions have been rejected by the chip card on the 2nd GAC. It appears that the terminal does not transmit the IAD correctly. It may truncate the IAD, which (in this case) have a length of 16 bytes, at 10 bytes and formatting the command of on the CDOL 2 is obliged to add 6 bytes padding.	
Terminal Information	Hypercom ICE 5500 in Ireland and Slovenia	
Corrective Action	Both acquirers have completed the fixed terminal deployment.	
Preventative Action	Preventative test case will be included in the next Test Plan version 4.1.b effective in November 2006.	
Additional Comments	None	

EMVCo Identifier	**I0061**	**Application Selection Error with B0'**
Date	Opened - November 8, 2005	Closed - April 8, 2009
Original Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ◓=MED	**Volume Severity** ○=LOW
Current Status	Pending Implementation – EMVCo, Payment System	**Field Implementation** ◓=SLOW _*Under Maintenance Mode_
Description	It was reported that some chip cards meet Off-line declines when they encountered some Ingenico terminals in France.	
Findings	A part of the ATR of some chip cards seem to be the same as the one in B0'application (French domestic application). Ingenico terminals installed in France perform the ATR checking for B0' application at the time of application selection in parallel with the AID selection processing. When transaction is performed with the above combination of the ICC and the terminal, transaction is terminated with "Carte Invalide" (i.e. Card Invalid) message before the payment system's application is selected. The ATR value for B0' is specifically fixed. French Terminal checks the ATR to determine whether the application is B0' or not. The Ingenico terminal behavior is as follows:	

	Step 1) Terminal checks if *MCF* is ***XX*** or not. If it is the case, terminal recognize that B0' application is to be selected and performed. Step 2) Terminal checks if the ATR is correctly set for B0' application or not. Terminal checks T0=***YY*** and MCH=***ZZ***. If it is the case, the B0' transaction is performed. If it is not the case, terminal recognizes that the ATR are incorrectly implemented and terminates the transaction. As certain chip has *MCF*=***XX*** and *MCH*=***not ZZ***, terminal understands that it is an error implementation for B0' application and terminates the transaction.
Terminal Information	Ingenico Elite series, I series, Ingeshop(In-house POS) in France (3 kernels)
Corrective Action	The terminal vendor has fixed the problem on the 3 kernels which have gone through the necessary testing process and is now ready for market implementation. Replacement has started with 158,000 terminals updated as of January 2009 - around 91% of the installed base. No field issues regarding this has been reported in over 12 months.
Preventative Action	This case has been reflected on the Best Practice on EMVCo website to call the attention of both acquirers/terminal vendors and issuers/bureaus. An Application Note regarding this issue is has been published.
Additional Comments	

EMVCo Identifier	I0060	**Transaction Severity** ●=HIGH
Issue Identifier	I0060	**Volume Severity** ●=HIGH
Status	Closed – EMVCo, Oct 24, 2006	
Date Opened	July 26, 2005	
Description	It was reported that some German cards met Online declines when they encountered some Bull and Ingenico terminals.	
Findings	It seems that some cards that use the PDOL to define the context of the transaction but also get data that will be later used for the cryptogram computation during the Generate AC. These data are typically the Transaction Currency Code or the terminal Country Code. Some terminals send 0x00s as part of the PDOL related data (GPO command data field) whereas the value is properly populated into the authorization message. When checked by the issuer the ARQC received in the authorization does not match the one recomputed, and result in Online declines.	
Terminal Information	Some Bull and Ingenico terminals in Turkey	
Corrective Action	5 acquirers in Turkey own the affected terminals. All acquirers have completed the terminal replacement and they have been confirmed by testing and live transaction monitoring.	
Preventative Action	Application Note has been published in July. Test cases have been released in May.	
Additional Comments		

EMVCo Identifier	I0055	**Transaction Severity** ●=HIGH
Issue Identifier	I0055	**Volume Severity** ●=HIGH
Status	Closed – EMVCo, PS 13 December 2005	
Date Opened	Oct 02, 2003	
Description	French B0'/EMV cards are rejected in UK terminals due to the change in convention at the Answer to Reset. At the ATR, the card initially responds using B0' protocol. The ICC data is presented in indirect convention (which is compatible with EMV) but with a specific protocol byte value not supported by EMV. The terminal is unable to process the response and issues a warm reset. Card now responds using an EMV compatible ATR but also changes to direct convention. The terminal is unable to recognize this change in convention.	
Findings	Acquirers are implementing various solutions (either correcting and upgrading the devices with a separate integrated PIN pad/reader, or replacing the devices). As of the end of 2004, a small percentage of devices remained to be upgraded.	
Terminal Information	Thales Cardmate2 XT52.	
Corrective Action	For these terminals, French B0'/EMV cards will fall back to magnetic stripe although there may be some inconvenience since the terminal will attempt to read the card three times prior to allowing fallback. (Update- May 18 2005): TAWG are sending letters to Vendors that failed and are going to fix the problems within a short time. Also, letters to other vendors have been sent by TAWG to make vendors aware of the problem. (Update- August 2005): TAWG has sent letters to the vendors that have failed the errata testing. (Update- December 2005) The only identified issue has been in the UK with the Thales terminals. It was confirmed that all the relevant terminals have been replaced in the field and corrective action has been completed.	
Preventative Action	EMVCo laboratories tested some of the earlier EMV96-approved IFMs for this 'change of convention' issue. Terminals were selected for sample retesting based on actual field deployment. The TAWG completed their testing and contacting vendors. The EMV2000 Level 1 approval process already tests for this condition.	
Additional Comments	None.	

EMVCo Identifier	I0057	**Transaction Severity** ◓=MED
Issue Identifier	I0057	**Volume Severity** ◓=MED
Status	Closed – EMVCo, PS July26, 2005	
Date Opened	May 05, 2004	
Description	SDA failure with cards containing a certificate based on an Issuer Public Key length of 1016-bits (127 bytes). In the reported incident, the terminal goes online, so the transaction is not declined.	
Findings	The cause of the problem may be related to the length of the Issuer Public Key (IPK) used to create the IPK Certificate. Some RSA cryptographic engines may exist that are not able to cope	

	with key lengths that are not evenly divisible by 16. The problem was isolated to one terminal type in the UK.
Terminal Information	Thales XT52 developed by and deployed in UK with application kernels 77148:02:07 and 77166:02:04. Corrected and approved in kernel 77166:03:00:00.
Corrective Action	The payment system advised Issuers accordingly and assessed the overall impact as 'moderate to low'. The vendor corrected the kernel and has received type approval. Acquirer testing and rollout of the correction was delayed in 2004 and will now carry over into 2005. (Update – May 18 2005) Terminal fix is available but has not been implemented in the field by Acquirers. Target date is to be determined.
Preventative Action	The test case is in place today. EMVCo will ensure that IPK lengths (in bits) that are divisible by 8 and not divisible by 16 will be tested as soon as possible. (Update- August 2005): TAWG confirmed that the relevant case will be covered in the new test cases (V3.5)
Additional Comments	None.

EMVCo Identifier	I0058	**Transaction Severity** ◓=MED
Issue Identifier	I0058	**Volume Severity** ●=HIGH
Status	Closed – EMVCo, PS (May 18 2005)	
Date Opened	December 01, 2004	
Description	An issue has been reported regarding the EMV specifications that do not specifically describe the process for retrying online PIN entry at an EMV device after the PIN fails validation on the first try. As a result, some Issuers assume a transaction restart after online PIN errors and decline the follow-on authorization request with a re-entered PIN if the second authorization request has the same Application Transaction Counter (ATC) as the first request. Acquirers have implemented various methods of handling PIN re-tries, and many devices retry the PIN validation without a transaction restart so the PIN retry request has the same ATC as the first request. This has caused unwarranted declines.	
Findings	The reported issue is an implementation issue best addressed by the payment systems. To further this work, the IWG reviewed this issue with JCB, MasterCard and Visa.	
Terminal Information	None.	
Corrective Action	CTWG responded to query.	
Preventative Action	None.	
Additional Comments	A Best Practices entry was published on the EMVCo website to advise Issuers of the possibility of such an occurrence and also to consider not to automatically decline solely due to duplicate ATC's in this circumstance.	

EMVCo Identifier	I0054	**Transaction Severity** ◒=MED
Issue Identifier	I0054	**Volume Severity** ○=LOW
Status	Closed – EMVCo, PS March 22, 2005	
Date Opened	Jan 8, 2004	
Description	It was reported that errors occur at certain terminals that set the TVR bit to 'PIN pad not present', even though the terminal supports PIN but has been deployed without a PIN pad and indicates non-support of PIN. A large number of Japanese and B0' cards are rejected. These cards are personalized to decline the transaction if PIN is requested but the PIN pad is not present.	
Findings	The terminal was being used without the features it was approved for. Attaching a PIN pad generated a different error due to an error in the software.	
Terminal Information	Ingenico TT41.	
Corrective Action	Solutions implemented by the Acquirer and vendor included the replacement/modification of the terminal in high traffic areas. Terminals were replaced in 2004 and into early 2005..	
Preventative Action	None.	
Additional Comments	Reference related issues I0033, I0053, and I0052.	

EMVCo Identifier	I0051	**Transaction Severity** ◒=MED
Issue Identifier	I0051	**Volume Severity** ●=HIGH
Status	Closed – EMVCo, PS – March 22, 2005	
Date Opened	Dec 30, 2003	
Description	It was reported that a high number of SDA failures occurred due to an error condition on the vendor's terminal.	
Findings	The SDA failure flag in the TVR is not being reset for the next transaction and will generate SDA failures until the device is powered off and back on. Depending on how the card has been personalized, the transaction will go online or be declined offline.	
Terminal Information	Thales Cardmate2.	
Corrective Action	The issue has been identified and there is a rollout plan for the correction. Acquirers will either apply the correction to the devices or will replace the devices. This is currently scheduled through the year 2004. As of February, almost all of the devices have been upgraded in the chip and PIN rollout.	
Preventative Action	Level 2 test case improvements were published in February. EMVCo requested that the test case implementation in the laboratories occur as expeditiously as possible.	
Additional Comments	None.	

EMVCo Identifier	I0049	**Transaction Severity** ●=HIGH
Issue Identifier	I0049	**Volume Severity** ◒=MED
Status	Closed – EMVCo, PS, June 3 2005	
Date Opened	Oct 02, 2003	
Description	It was reported that a terminal type issued a Get Data for the Pin Try Counter even when the offline PIN CVM was not present on the card. The card responds with an error code and goes into an idle state causing the terminal to terminate.	

Findings	The POS terminal issues a Get Data Pin Try Counter prior to a read and analyze of the CVM list. The cards were personalized to not support offline PIN CVM.
Terminal Information	Dione Exchequer (POS with PIN pad).
Corrective Action	The terminal software was changed to only issue Get Data for the Pin Try Counter when the card supports offline PIN.
Additional Comments	No more information on possible incident in France.
Additional Comments	None.

EMVCo Identifier	I0046	**Transaction Severity** ●=HIGH
Issue Identifier	I0046	**Volume Severity** *N/A*
Status	Closed – EMVCo, PS Jan 30, 2004	
Date Opened	Sep 03, 2003	
Description	It was reported that a European card did not include the tag for the unpredictable number in the CDOL2, as required in EMV Specifications Update #6. The potential error would cause a CDA failure and transaction decline.	
Findings	Specifications Update Bulletin #6 requires that for CDA transactions, the Unpredictable Number be in both CDOL1 and CDOL2. This assures that if the terminal generates a different Unpredictable Number for the second Generate AC than that used in the first Generate AC, the card will receive this new value and use it in generating the application cryptogram and the signed dynamic application signature. If the CDOL2 does not include the Unpredictable Number, the CDA will fail and the transaction will be declined.	
Corrective Action	The Issuer notified EMVCo of the issue. CDA will not be implemented until the cards are corrected.	
Preventative Action	The Security Working Group reviewed the issue and determined that no additional clarification was needed to the specifications.	
Additional Comments	None.	

EMVCo Identifier	I0044	**Transaction Severity** ●=HIGH
Issue Identifier	I0044	**Volume Severity** ○=LOW
Status	Closed – EMVCo, PS July 27, 2004	
Date Opened	Jul 14, 2003	
Description	It was reported that terminals were incorrectly processing offline data authentication for cards with the same length Issuer Public Key and the CA Public Key used.	
Findings	EMV 4.0 allows the Issuer Public Keys to be equal to or shorter than the CA Public Keys. However, EMV 3.1.1 specifies that the length of the Issuer Public Keys should be shorter than the CA Public Keys. As a result, offline data authentication failures could occur due to same length IPK and CA PK. Several older models of devices were identified to have this problem. Issuers are impacted if they personalize their cards to decline transactions based on the failure of offline data authentication.	
Corrective Action	The vendors were notified, and the payment system confirms that the issue is now resolved.	
Preventative Action	Type Approval testing now checks for this condition.	
Additional Comments	None.	

3.13 Closed -- Payment System Activities Complete

EMVCo Identifier	**I0072**	**IAD not beginning with length byte**
Date	Opened – Feb 02, '08	Closed – June 24, '08
Original Assessment	**Transaction Severity** ◒=MED	**Volume Severity** ◒=MED
Current Assessment	**Transaction Severity** ○=LOW	**Volume Severity** ○=LOW
Current Status	Pending Implementation – Payment System	**Field Implementation** ◒=SLOW
Description	Some Ingenico terminals used in Canada are unable to correctly transit certain formats of Issuer Application Data (IAD) to acquirer. The terminal always sends a full 32 byte of IAD regardless of the length of IAD received from card. When IAD is not beginning with length byte, the acquirer either is unable to determine the IAD which causes an error at the acquirer or determines an incorrect IAD which causes cryptogram validation failure at the issuer host.	
Findings	The problem is in the local application layer and not in the approved kernel. Impacted Terminals: 72,000 in Canada Impacted Cards: Cards with IAD that is less than 32 byte and not carried in two parts with each part beginning with a length byte.	
Terminal Information	Ingenico	
Corrective Action	A Fix is available and being applied to all terminals. Further investigation revealed that there were no affected cards due to the nature of the payment system's card specifications. In light of the above, this issue is considered closed.	
Preventative Action	None	
Additional Comments		

EMVCo Identifier	**I0071**	**Leap Year Day Issue – 2**
Date	Opened - Feb 26, '08	Closed – Feb 03, 2009
Original Assessment	**Transaction Severity** ◒=MED	**Volume Severity** ●=HIGH
Current Assessment	**Transaction Severity** ◒=MED	**Volume Severity** ○=LOW
Current Status	Pending Implementation – Payment System	**Field Implementation** ◒=SLOW ***Under Maintenance Mode***
Description	The Diebold ATMs which have issues handling cards with expiration date set with leap year day of 2012/2/29 and 2016/2/29. Transaction is terminated offline.	
Findings	The problem is in application layer component and not in the approved kernel. The application layer component did not handle and manage correctly the leap year of February 2012. All the internal tests of the application component have been performed with leap year of 2008.	
Terminal Information	What is common to all possibly impacted applications : - They have the Diebold Emv Kernel 4.0 (EMVCo specs), (Build Release 3.1.0.2).	
Corrective Action	Hot fix has been developed and is available on the centralized server which Acquirers can download and install. Released on Oct 26th, 2007.	
Preventative Action	Test case exists in the Test Plan v4.1.b.	
Additional Comments		

EMVCo Identifier	**I0070**	**ICC Public Key >= 1024 bit in Format 1**
Date	Opened - Feb 6, 2007	Closed – April 30, 2013
Original Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ●=HIGH
Current Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ○=LOW
Current Status	Pending Implementation – Payment System	**Field Implementation** ◓=SLOW **Under Maintenance Mode*
Description	Certain terminals in the field are either wrongly failing DDA, or terminating transactions when the DDA card's ICC Public Key is greater than or equal to 1024 bits and respond to INTERNAL AUTHENTICATE using Format 1. Similarly, certain terminals in the field are wrongly failing CDA when the card's ICC Public Key is greater than or equal to 1024bits.	
Findings	There is a problem with certain DDA-supported terminals when a card's ICC Public Key is greater than or equal to 1024 bits. When the card responds to the INTERNAL AUTHENTICATE command using Format 1, DDA supported terminals either fail DDA, or terminate the transaction. This issue occurs because the length field of the INTERNAL AUTHENTICATE response is two bytes long when the key is 1024 bits or more. Certain CDA supported terminals were not handling two byte length encoding of the dynamic signature tag (tag 0x9F4B). Since the length for the dynamic signature tag was read wrongly, the dynamic signature was calculated wrongly and hence CDA failed. In summary, these terminals cannot process the two-byte length field in the response and/or in Tag 9F4B. When the ICC Public Key is less than 1024 bits, the length field of the response and Tag 9F4B is one byte. These same terminals can properly interpret the single byte length, so no error occurs. DDA supported terminals can also successfully process the response data in Format 2 containing ICC Public Keys of 1024 bits or greater. This issue has been identified in Taiwan, UAE, Brazil, Malaysia, New Zealand, Hong Kong, UK, and Ireland.	
Terminal Information	<DDA Issue> Hypercom (v4.16~v4.18 kernels) and VeriFone terminals (Verix 2.0/2.1.1, Verix V 2.0/2.1, Vx SE EMV Module 1.0). <CDA Issue> VeriFone terminals (Verix 3.0, Verix V 3.0, SC5000 2.0/2.1)	
Corrective Action	Hypercom: Replacement for new kernel version 5.x series has started. Verifone: Kernel fixes have been developed (Verix 2.0.5/2.1.5, Verix V 2.0.5/2.1.5, Vx SE EMV Module 1.0.1) and replacement has started. Their new kernel range, version 3.x series (Verix 3.0.5, Verix V 3.0.5) are also ready for replacement. The terminal upgrades in Europe are scheduled to be completed in the next few months.	

Preventative Action	TA Bulletin became effective April 20th, 2007. Test Plan version 4.1.c effective May 2007.
Additional Comments	Problematic kernels have been removed from the EMVCo Approval List and replaced with the fixed kernels where appropriate. CLOSED due to no new issues being reported for over 12 months with limited (low) terminals/cards affected.

EMVCo Identifier	**I0066**	**Leap Year Day Issue**
Date	Opened - Sep 19, 2006	Closed - July 20, 2010
Original Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ○=LOW
Current Status	Pending Implementation – Payment System	**Field Implementation** ○=GOOD
Description	It has been reported that there are issues with terminals not being able to handle cards with expiration date set with leap-year-day for specific dates.	
Findings	Certain Gemalto terminals are not able to handle cards with expiration date set with 29 Feb 2012 and 2016, and terminate the transaction.	
Terminal Information	Affected Gemalto terminals are located in UK, France, Italy, Greece, Croatia, Balkan countries, India, Thailand, Malaysia, South Africa.	
Corrective Action	Fixed kernels are now available and market deployment has begun. Balkans /Croatia /Malaysia /Thailand /UK /Italy /South Africa – 100% complete, India – 80 % complete, Greece – 86% complete, France – 100% complete, Not started or No information – Turkey.	
Preventative Action	Preventative test case has been included in Test Plan version 4.1.b effective as of November 2006.	
Additional Comments	Known terminals have been fixed, no new field incidents reported in the last 12 months – this issue is closed.	

EMVCo Identifier	I0063	**Transaction Severity** ●=HIGH
Issue Identifier	I0063	**Volume Severity** ◓=MED
Status	Closed – EMVCo	
Date Opened	July 07, 2006	
Description	It was reported that some terminals do not manage the IAD (Issuer Authentication Data) correctly if the length of the data received in the authorization response is shorter than the one requested for the second Generate AC command (CDOL2).	
Findings	In such case the terminal is obliged to manage the right padding but the padding is not always correctly managed (left padding) resulting in rejection of the transaction by the card. There is no risk for domestic transactions as French issuers are not using such mechanism.	
Terminal Information	Some Wincor ATM in France	

Corrective Action	So far 600 affected ATMs have been replaced. There are currently 171 remaining affected ATMs all of which do not have any cross border transactions. We have been informed the bank does not plan to upgrade these ATMs unless they experience field issues at these ATM locations. The IWG have agreed to close this issue.
Preventative Action	Preventative test case has been included in Test Plan version 4.1.b effective as of November 2006.
Additional Comments	

EMVCo Identifier	**I0059**	**Instability of Vcc during I/O Transitions**
Date	Opened - April 18, 2005	Closed - Feb 03, 2009
Original Assessment	**Transaction Severity** ●=HIGH	**Volume Severity** ◓=MED
Current Assessment	**Transaction Severity** ○=LOW	**Volume Severity** ○=LOW
Current Status	Pending Implementation – Payment System	**Field Implementation** ◓=SLOW _*Under Maintenance Mode_
Description	When inserted into a Moneyline S3000/L3000 terminal, several cards using Infineon chip from family (SLE66Cx2P) do not occasionally start, due to an electrical incompatibility.	
Findings	It seems that the terminal does not sufficiently stabilize the Vcc during I/O transitions when communicating with the Infineon chip, resulting in peak over the security sensor implemented by the card (even though the chip has implemented some buffer above the specified maximum voltage described in the EMV specification). This issue does not always happen with the same terminal and chip card but happens in 6-10 % of the transactions. By changing the capacitor, the failure rate goes down to about 1%.	
Terminal Information	Moneyline terminals installed in France have been affected	
Corrective Action	Affected terminals in large major retailers have been replaced. The rest of terminals are being fixed in their yearly maintenance process and on ad hoc basis based on merchant request. 40% of all terminals has been replaced. The fixed new IFM has been approved, and the old IFM will be removed from Level 1 IFM approval list on the website.	
Preventative Action	The communication memo was issued to all the EMVCo accredited laboratories to call their attention to this issue in June 2006 as the Laboratory Memo #62.	
Additional Comments		

EMVCo Identifier	**I0056**	**URL in Issuer Discretionary Data**
Date	Opened - April 2, 2004	Closed - Feb 03, 2009
Original Assessment	**Transaction Severity** ○=LOW	**Volume Severity** ○=LOW
Current Assessment	**Transaction Severity** ○=LOW	**Volume Severity** ○=LOW
Current Status	Pending Implementation – Payment System	**Field Implementation** ●=NO UPDATE _*Under Maintenance Mode_

Description	A terminal type was unable to handle the Issuer URL (tag '5F50') returned in the FCI Issuer Discretionary Data (tag 'BF0C') on a SELECT command. "Card Data Error (0200)" message was received.
Findings	The terminal should ignore unrecognized data elements. In this case, the terminal 'hangs' and is unable to continue processing. The terminal software will be changed in a subsequent release. No new reports of card failures have been reported. Payment systems are working with their members to identify and correct the error for the cases in Sweden. There are 1000 terminals that are affected in Sweden. Another incident has been reported in Czech Republic, where 10,000 terminals are being affected. The payment system has instructed the sole acquirer of these terminals within Czech Republic not to deploy any new terminals that reject the cards with URLs.
Terminal Information	Ingenico Elite 510T (Unicapt 16 kernel) in Sweden and Czech Republic.
Corrective Action	The terminal vendors have been replacing the terminal prioritizing on high volume merchants. Swedish terminal replacement complete, Czech terminal replacement has started and 6500 terminals have been replaced. The rest will be replaced in the regular maintenance mode.
Preventative Action	Application Note #20 regarding 'Additional Data Allowed in the Directory Discretionary Template' was published in April 2004. If the terminal encounters data elements that are not understood or recognized, the elements should be ignored. The new Test Plan has already included the relevant test case. This kernel has been revoked from the EMVCo website.
Additional Comments	Very few cards are affected, less than 0.5% of all transactions at these terminals may be affected by this issue.

EMVCo Identifier	I0053	**Transaction Severity** ◒=MED
Issue Identifier	I0053	**Volume Severity** ○=LOW
Status	Closed – PS , July 27, 2004	
Date Opened	Jan 8, 2003	
Description	It was reported that some terminals may have problems processing an 1152-bit CA key. Terminals properly store the key, but processing of the larger certificate during a transaction results in a failure. Depending on how the card has been personalized, the SDA/DDA failures cause the transaction to be declined offline or go online for authorization.	
Findings	These are earlier pre-EMVCo terminals in the field.	
Corrective Action	The terminals, as they are identified, will be upgraded.	
Preventative Action	None.	
Additional Comments	Reference related issues I0054, I0052, and I0033.	

EMVCo Identifier	I0052	**Transaction Severity** ◓=MED
Issue Identifier	I0052	**Volume Severity** ○=LOW
Status	Closed – PS , July 27, 2004	
Date Opened	Dec 30, 2003	
Description	It was reported that SDA failures consistently occur on a small number of a vendor's devices (50 out of approximately 100,000).	
Findings	Depending on how the card has been personalized, the SDA failures cause the transaction to be declined offline or go online for authorization. Cardholder impact is minimal. The payment systems currently recommend to not decline offline on such an SDA error.	
Corrective Action	The terminals will be reconfigured or replaced in the chip and PIN rollout in 2004.	
Preventative Action	None.	
Additional Comments	Reference related issues I0054, I0053, and I0033.	

EMVCo Identifier	I0042	**Transaction Severity** ◓=MED
Issue Identifier	****	**Volume Severity** ◓=MED
Status	Closed – PS, Mar 7, 2003	
Date Opened	Jan 31, 2003	
Description	It was reported that newly certified and issued cards were being rejected with a message, 'application not yet effective', at particular terminals.	
Findings	It was determined that the error occurred only on certain terminals. Transactions are forced online to the Issuer for authorization. A modification was made to the Acquirer's host application for reading of the chip data.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	For EMVCo informational purposes only.	

EMVCo Identifier	I0040	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ◓=MED
Status	Closed – PS, Oct 1, 2002	
Date Opened	Jul 10, 2002	
Description	It was reported that a terminal approved all transactions offline, even under conditions that the terminal floor limit was set to zero.	
Findings	This was an issue with the terminal implementation. The vendor corrected the software and released a new software version. Terminals have been corrected.	
Corrective Action	The vendor has corrected the terminal application.	
Preventative Action	None	
Additional Comments	For EMVCo informational purposes only.	

EMVCo Identifier	I0039	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – PS, Jul 22, 2003	
Date Opened	Jul 4, 2002	
Description	It was reported that ICC cards were not accepted by a particular terminal type.	
Findings	These were about 200 older terminals in the field. They have either been replaced by approved terminals, removed, or EMV-disabled for chip.	
Corrective Action	Terminals have been replaced.	
Preventative Action	None.	
Additional Comments	For EMVCo informational purposes only.	

EMVCo Identifier	I0037	**Transaction Severity** *N/A*
Issue Identifier	I0037	**Volume Severity** *N/A*
Status	Closed – PS, May 23, 2003	
Date Opened	Dec 15, 2002	
Description	It was reported that cards used at a particular terminal application were unable to successfully perform Issuer Authentication.	
Findings	It was determined that the terminal was improperly extracting the response code for return to the card. The card was therefore unable to authenticate the response cryptogram.	
Corrective Action	The vendor has corrected their terminal application.	
Preventative Action	None.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0035	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – PS, Jan 22, 2003	
Date Opened	Oct 4, 2002	
Description	It was reported that cards used at a particular terminal application were unable to successfully perform Issuer Authentication.	
Findings	It was determined that the Acquirer did not support the full data chip option. As a result, a response cryptogram was not returned to the card that prevented it from successfully performing Issuer Authentication. In this instance, the rejected cards had been configured to decline the transaction if Issuer Authentication could not be performed.	
Corrective Action	Issuers have been advised not to configure their cards to decline if Issuer Authentication is not performed.	
Preventative Action	None.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0034	**Transaction Severity** N/A
Issue Identifier	****	**Volume Severity** N/A
Status	Closed – PS, Feb 21, 2003	
Date Opened	Oct 26, 2002	
Description	A technical inquiry was submitted relative to the need for certain cards to support different Cardholder Verification Methods (CVM) for both credit and debit application.	
Findings	The inquiry was responded to and referred to the payment system. This was a customization and card personalization question that has been resolved.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0033	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ●=HIGH
Status	Closed – PS, July 27, 2004	
Date Opened	Oct 11, 2002	
Description	Interoperability problems were being experienced on an older terminal.	
Findings	It was determined that the terminal application was not EMVCo-approved. The terminal application must be submitted for EMVCo approval.	
Corrective Action	The device has now gone through approvals. Acquirers are working with the vendor to get the older devices replaced in 2004 with approved chip and PIN devices.	
Preventative Action	None.	
Additional Comments	Reference related issues I0054, I0053, and I0052.	

EMVCo Identifier	I0032	**Transaction Severity** ○=LOW
Issue Identifier	****	**Volume Severity** ◓=MED
Status	Closed – PS, Nov 13, 2002	
Date Opened	Oct 11, 2002	
Description	It was reported that Issuer script commands were not being properly processed.	
Findings	It was determined that the terminal-to-acquirer messages did not support issuer scripts that exceeded 24 bytes. EMV allows for Issuer script data to include as many as 128 bytes.	
Corrective Action	This is a potential problem with the interoperability of scripts from non-UK Issuers being truncated by UK Acquirers. For information only.	
Preventative Action	None.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0028	**Transaction Severity** N/A
Issue Identifier	****	**Volume Severity** N/A
Status	Closed – PS, Nov 22, 2002	
Date Opened	Oct 4, 2002	
Description	It was reported that some cards were not being accepted at particular ATM devices.	

Findings	It was determined that the ATMs were not configured to support the AID encoded on the card. The acquirer needs to ensure that terminals contain the AIDs for the applications accepted by the ATM.
Corrective Action	The devices were corrected and the issue resolved.
Preventative Action	None.
Additional Comments	This is not an EMV issue.

EMVCo Identifier	I0020	**Transaction Severity**	N/A
Issue Identifier	****	**Volume Severity**	N/A
Status	Closed – PS, Nov 22, 2002		
Date Opened	Oct 4, 2002		
Description	It was reported that some cards were failing in particular terminal applications.		
Findings	It was determined that the rejected cards were personalized with an AID and suffix. However, the terminal software did not support the partial AID selection that is required when the AID has a suffix. This is an EMV terminal requirement.		
Corrective Action	The payment systems are managing the issue. The temporary solution was to have a phased re-issuance of earlier cards (with the suffix). This has been completed.		
Preventative Action	None.		
Additional Comments	This is not an EMV issue.		

EMVCo Identifier	I0019	**Transaction Severity**	●=HIGH
Issue Identifier	****	**Volume Severity**	●=HIGH
Status	Closed – PS, Nov 29, 2002		
Date Opened	Oct 4, 2002		
Description	It was reported that some cards were failing in a particular terminal application.		
Findings	It was determined that the terminal application was timing-out during the Answer to Reset due to the slower processing and response time of the card.		
Corrective Action	The identified chip card will be phased out of usage and has already been removed from the list of approved suppliers. The payment systems are managing this issue, and the last cards will expire August 2004. Terminal vendors have made changes to their devices to accommodate the slower cards.		
Preventative Action	None.		
Additional Comments	This is not an EMV issue.		

EMVCo Identifier	I0018	**Transaction Severity**	○=LOW
Issue Identifier	****	**Volume Severity**	○=LOW
Status	Closed – PS, Nov 29, 2002		
Date Opened	Oct 4, 2002		
Description	This was a technical request to modify the EMV specifications to change the formatting of the Issuer Application Data field originating from the card.		
Findings	No change will be made to the specifications. Changing the existing format for data transport would impact all existing Issuers and Full Data Option Acquirers.		

Corrective Action	None.
Preventative Action	None.
Additional Comments	This is not an EMV issue.

EMVCo Identifier	I0017	**Transaction Severity** ◓=MED
Issue Identifier	****	**Volume Severity** ◓=MED
Status	Closed – PS, Nov 29, 2002	
Date Opened	Oct 4, 2002	
Description	It was reported that some cards were unable to successfully perform Issuer Authentication when used with a particular terminal application.	
Findings	It was determined that card declines were occurring due to the payment system's conversion of ASCII to EBCDIC characters. This conversion resulted in the card's inability to successfully perform Issuer Authentication. The payment system reviewed the concern. Changing the format in the network system would impact all existing Issuers and Full Data Option Acquirers. No change will be made.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0014	**Transaction Severity** ○=LOW
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – PS, Nov 22, 2002	
Date Opened	Jan 14, 2002	
Description	It was reported that cards could be issued with keys that expired prior to the card expiration date. This was identified as a potential problem – not one currently being experienced.	
Findings	It was determined that this was a card personalization issue that would need to be managed by the payment system.	
Corrective Action	None.	
Preventative Action	None.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0009	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – PS, Nov 29, 2002	
Date Opened	Aug 27, 2002	
Description	It was reported that some non-domestic cards were being rejected by a terminal application in Brazil.	
Findings	It was determined that the terminal application in question was non-EMV compliant.	
Corrective Action	The terminal application is being upgraded to an EMV-compliant version. Chip migration of devices is scheduled to be complete by March 2004.	
Preventative Action	The payment systems will ensure that all deployed terminal applications are EMV-compliant.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0008	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ○=LOW
Status	Closed – PS, Feb 23, 2003	
Date Opened	Oct 10, 2002	
Description	It was reported that the request cryptogram (ARQC) originating from cards used with a particular terminal application was invalid.	
Findings	It was determined that a terminal application was deployed in a Hotel T&E environment where the transaction amount was changed at the time of check out. The transaction amount used in the request cryptogram was different from the amount in the online authorization.	
Corrective Action	The terminal application was modified to transmit the correct transaction amount. As of February 2004, the majority of devices were corrected. However, there are still a few errors and the Acquirer is reviewing the issue. The ongoing review of these CAM errors will be managed and addressed by the payment system.	
Preventative Action	None.	
Additional Comments	This is not an EMV issue.	

EMVCo Identifier	I0003	**Transaction Severity** ●=HIGH
Issue Identifier	****	**Volume Severity** ●=HIGH
Status	Closed – PS, Nov 22, 2002	
Date Opened	Aug 27, 2002 & Oct 4, 2002	
Description	Various errors were being experienced with a particular terminal application related to the processing of the Card Verification List (CVM).	
Findings	It was determined that the terminal application in question was not EMVCo-approved.	
Corrective Action	The vendor corrected the terminal application and the payment systems are managing the rollout of the approved updates. All corrections and downloads to devices were completed in 2003.	
Preventative Action	None.	
Additional Comments	This is not an EMV issue.	

***** END OF DOCUMENT *****