EMV DUAL INTERFACE CHIP
CARD PERSONALIZATION VALIDATION REPORT

CPV INFORMATION

CPV Reference Number	CPV_FIM_181015_083405
Report Date	14-Jan-19
Report Type	☐ SSF ☐ Card Image ☒ Sample Card
Report Version	Iteration: 2 - Report version: b
Customer Name	Cetelem
Customer Country	Portugal
Mastercard Brand	Mastercard
Device Type	Card
BIN(s)	528069
Mastercard Project Number	N/A

IMPORTANT NOTE

This report, when duly signed by the Mastercard representative, indicates a successful completion of the CPV service for the submitted Sample, and allows the issuer to deploy chip products corresponding to that Sample for the applicable BIN(s) or BIN range(s), subject to any restriction mentioned.

When NOT signed by the Mastercard representative this report only indicates that Sample Submission Form, Card Image or Sample you have submitted has been validated by your Service Provider. Please refer to the Validation Results section to find out whether this validation was successful or unsuccessful.

MASTERCARD REPRESENTATIVE SIGNATURE

Title	**Name, Signature & Date**
Mastercard Representative Signature	Paul Vanneste Digitally signed by Paul Vanneste DN: cn=Paul Vanneste, o=Mastercard, ou=EMV & Digital Devices, email=paul.vanneste@mastercard.com, c=BE Date: 2019.01.17 16:40:05 +01'00'

Template Version: EMV Dual Interface Chip v7.3

MASTERCARD DISCLAIMER

This **EMV Dual Interface Chip Card Personalization Validation Report** (CPV Report) has been provided to Mastercard Worldwide (“Mastercard”) by your Service Provider. When duly signed by the Mastercard representative, it indicates that your product has successfully passed the Mastercard required Card Personalization Validation testing as defined on the basis of the Specification References information listed in the Information section hereafter.

Under no circumstances does this CPV Report include any endorsement or warranty regarding the functionality, quality or performance of any other product or service provided. Under no circumstances does this CPV Report include or imply any product or service warranties from Mastercard, including, without limitation, any implied warranties of merchantability, fitness for purpose, or non-infringement, all of which are expressly disclaimed by Mastercard. All rights and remedies regarding Customer Service Provider’s products, services and Customer’s services for which Mastercard has granted this CPV Report shall be provided by the party offering such products or services and not by Mastercard.

Please note that:

- Unless otherwise specified in the Validation Results section of this CPV Report, the testing performed only covers data readable from the cardholder device. It does not cover internal data.
- This report does not intend to cover the embossing and the encoding nor data that are not specifically linked to the EMV chip technology (for instance, the value of the PAN or Cardholder Name as embossed on the card or the value of the second and third position of the service code).
- Regarding the Track 1 and Track 2 Data, only the consistency of the magnetic stripe and chip data is; not all the detailed values of each sub-data are reviewed. For example, consistency of the various values of the cardholder name, expiration date and service code are tested but not the value of the PVV.
- Unless otherwise specified in the Summary Test Results section, no dynamic tests (Transaction Certificate generation, PIN verification, etc) are part of the testing. Therefore internal data, mandatory for a transaction, may be missing even in case of a successful CPV Report. When conclusions of dynamic tests are specified in the Summary Test Results section, they refer to simple dynamic tests (for Full Chip issuers: Transaction Certificate validation and Change PIN command; for Magstripe Grade issuers: 50 online transactions without issuer authentication and with ARC set to “00”). These dynamic tests do not provide full evidence that all internal data mandatory for a transaction are present in the cardholder device.
- As an on-going effort to enhance the approval process, Mastercard may add or update from time to time the tests performed during the Chip Personalization Validation. This means that a sample having received a successful CPV Report may receive an unsuccessful CPV Report if resubmitted at a later time.
- As an on-going effort to enhance cardholder device acceptance and security, Mastercard may modify its specifications as a result of field experience or in order to introduce improved features. Despite Mastercard best efforts to ensure backward compatibility when introducing such modifications, this means that a sample having received a successful CPV Report may receive an unsuccessful CPV Report if resubmitted at a later time.
- The testing validates the compliance of the submitted item with the requirements defined in the specifications mentioned in the Information section, without any reference to any other previous submission.

EMV DUAL INTERFACE CHIP
CARD PERSONALIZATION VALIDATION REPORT

CPV INFORMATION

CPV Reference Number	CPV_FIM_181015_083405
Report Date	14-Jan-19
Customer Name	Cetelem
Customer Country	Portugal
Mastercard Brand	Mastercard
Device Type	Card
BIN(s)	528069
Mastercard Project Number	N/A
CPV Service Provider	FIME

VALIDATION TYPE

Sample Submission Form	Card Image	Sample Card
☐	☐	☒

PERFORMED BY

Title	**Name, Signature & Date**
CPV Operator	Joyce Du I am the author of this document 2019-01-16 14:26+08:00

CONTROLLED & APPROVED BY

Title	**Name, Signature & Date**
CPV Supervisor & Quality Manager	Eugene Sung I have reviewed this document 2019.01.16 14:29:46 +08'00'

SERVICE PROVIDER DISCLAIMER

FIME has analyzed the data and/or card samples provided by the Customer in strict conformance with the Mastercard recommendations as stipulated in the requirements provided to service providers applicable at the time when this report was issued. The results of this analysis have been summarized in this **EMV Dual Interface Chip Card Personalization Validation Report** (CPV Report) and signed by Mastercard under the terms of FIME’s accreditation under the Mastercard “Formal Approval Services” accreditation.

It shall be noted however that the terms of the Mastercard disclaimer as stated on page 1 of this report , and which are related to technical data (specifically the bullet items following the statement: “Please note that”) apply equally to FIME and to Mastercard.

In addition, it shall be noted that:

- when a “pre-validation” or “paper validation” is performed based on the Customer generated values listed in the Sample Submission Form (SSF), it must be understood that a successful result does not ensure that the CPV performed on the Card Image files and/or card sample will be successful because additional data, such as dynamic data, cannot be verified in the preliminary validation.
- FIME provides the card sample analysis report based on the assumption that these are pre-production samples. FIME cannot be held liable for any and all changes made by the Customer to the card personalization setting after issuance of the CPV Report.

FIME will perform the CPV with all due care and in accordance with the state of the art as defined by the Mastercard and EMVCo specifications and associated test requirements. However, FIME cannot be held liable for, and specifically declines, responsibility or liability for performance issues not explicitly addressed in these Mastercard and EMVCo specifications and associated test requirements, including, but not limited to, interoperability issues. Deliverance of the report to Mastercard does not imply any warranties or implied warranties or merchantability, fitness for purpose, or non-infringement, all of which are expressly disclaimed by FIME.

TABLE OF CONTENTS

INFORMATION

I.	**Service Provider Test Location**			Taipei Taiwan
II.	**Tool Identification**			PersevalPro Issuer - CPV 11.3
III.	**Test Session**	Date:		14-Jan-19
		CPV Result Filename:		RES_CPV_FIM_181015_083405_ALL_2.xml
		Profile File Reference		N/A
		Profile Rule Set Version		N/A
IV.	**Sample Identification**	PAN:		528069 xxxxxx 6002
		Cardholder Name:		AKEJNOPMA SYVKYQ/
		Expiration Date:		31-Dec-21
V.	**Specification References**	**Normative References**	[FA]	M/Chip Requirements for Contact and Contactless [Nov 2017]
		M/Chip Advance	[MCA]	M/Chip Advance Card Application Specification – Payment & Data Storage [v1.2.1 - Aug 2016] M/Chip Advance Product Derivation [Version 1.2.2 – Oct 2017]
			[PDS]	M/Chip Personalization Data Specifications for Contact and Contactless [March 2018]
			[IG]	M/Chip Advance Issuer Guide v2.2.1 [October 2017]

VALIDATION RESULT

Validation Result:	Successful

For a non-successful validation result, refer to the Issue List section for the errors to be corrected. These are flagged as ‘Errors’ in the Issue List

Restrictions:

Conditions of Approval

1. M/Chip Advance 1.2 is equivalent to M/Chip Advance 1.1 after personalization if 1.2 specific features are not activated.
2. The Vendor has confirmed backward compatibility of this product with personalization scripts developed for their previous v1.1 product. Such a 1.1 script will not activate 1.2 specific features. Note that MasterCard Type Approval process does not cover this point.

TAS Comments

The Cold ATR is not a basic one as defined by the EMV specification; it contains TA1='13' and TA2='80' (No negotiable specific mode), which means that the card supports a high speed transfer rate. The card protocol evaluation covers both transfer rates 9600bits/s and 38400bits/s. But there is a risk that some terminals use the negotiation mechanism during an EMV transaction without being able to properly identify a proprietary context (card from a specific bank into a terminal from the same bank or from the same country...) for which the EMV specification allows the usage of additional mechanisms. MasterCard cannot guarantee that every terminal will skip this negotiation phase. This mechanism is beyond the scope of EMVCo and MasterCard approval. Therefore there is no guarantee that both implementations - card side and terminal side - will be interoperable.

Dynamic CVC3 verification

The dynamic CVC3 verification has not been performed because the IMKcvc3 has not been provided. The CVC3track1 and CVC3track2 generated values are different. However, it is not possible to ensure that Dynamic CVC3 calculation is compatible with Mastercard recommended method. Mastercard recommends the Issuer to perform End to End tests including dynamic CVC3 validation before deployment. As per Global Operations Bulletin No. 11, 1 November 2016, the issuer, out of the U.S. Region, must adopt the Dynamic CVC3 Validation in Stand-In Processing service as of 1 April 2017 using Mastercard recommended method. As per the U.S. Region Operations Bulletin No. 8, 11 April 2017, the issuer, in the U.S. Region, must adopt the Dynamic CVC3 Validation in Stand-In Processing service as of 1 July 2017 using Mastercard recommended method.

Application Label

The Application Label stored in the card contains the values [MC Predefi], [MC 3x com], [MC 12x com], [MC 24x com] whereas for the Mastercard applications with extended AID, the Application Label must start with "Mastercard" or "MASTERCARD" and contain additional text that makes it distinguishable from all other applications. However, according to CHIP_22952 email, Mastercard has exceptionally agreed to accept the current Application Labels.

Application ID (Tag 4F) in PPSE

PIX extensions should not be used in the AID on the contactless interface as some legacy contactless terminals do not support partial AID matching. If the same account is accessed through the contact and contactless interfaces, the AID used on each interface might be different; the contact AID may contain a PIX extension, but the contactless AID excludes this PIX extension.
However, according to email on date [10-Jan-2019] from [Anabela Duarte <Anabela.Duarte@sibs.pt>], the issuer is willing to take responsibility for any interoperability issue entailed to using an extended AID on the Contactless interface.

Notes:

None

Product Approval Validation

Letter of Approval:	CLOA-OBTR170901-171103 which expires on 24-Aug-20[1]
Chip Vendor:	OBTR-Colombes
Chip Model:	MCADDS v1.2.1 Cosmo Fly v6.0 MCADDS 01 Infineon SLC32PDL348 / h13
Product Personalization Validation	
Primary brand:	Mastercard
Issuer given card name:	Combo
Special Program:	☐ Prepaid ☐ Unembossed ☒ None ☐ Other:
Personalized by:	SIBS Cartões
Application Profile Validation: Mastercard (AID A0000000041010AA04)	
Reference Profile:	Chip Grade - Offline PIN, Online PIN, Signature and No CVM
Offline CAM:	DDA - CDA
Standard Profile:	No
Online Profile:	Offline capable
Geographical Acceptance:	Domestic & International
Application Profile Validation: Mastercard Contactless (AID A0000000041010AA04)	
Reference Profile:	Online PIN, Signature and No CVM
Offline CAM:	CDA only
Standard Profile:	No
Online Profile:	Offline capable
Geographical Acceptance:	Domestic & International
Contactless Technology:	EMV Contactless And Mag-stripe Contactless
Application Profile Validation: Mastercard (AID A0000000041010AA01)	
Reference Profile:	Chip Grade - Offline PIN, Online PIN, Signature and No CVM
Offline CAM:	DDA - CDA
Standard Profile:	No
Online Profile:	Offline capable

[1] It is the responsibility of the issuer to ensure that cards issued are covered by a valid Letter of Approval, or that the product is in the process of having its Letter of Approval renewed.

Geographical Acceptance:	Domestic & International
Application Profile Validation: Mastercard (AID A0000000041010AA02)	
Reference Profile:	Chip Grade - Offline PIN, Online PIN, Signature and No CVM
Offline CAM:	DDA - CDA
Standard Profile:	No
Online Profile:	Offline capable
Geographical Acceptance:	Domestic & International
Application Profile Validation: Mastercard (AID A0000000041010AA03)	
Reference Profile:	Chip Grade - Offline PIN, Online PIN, Signature and No CVM
Offline CAM:	DDA - CDA
Standard Profile:	No
Online Profile:	Offline capable
Geographical Acceptance:	Domestic & International

SUMMARY TEST RESULTS

For each test failed, the ‘Issue List’ section provides details of the issues identified. Unless explicitly mentioned, the remarks apply to both the contact and contactless interfaces.

Primary Application: Mastercard (AID A0000000041010AA04)		
Test	**Test Scope**	**Test Result**
ICC Track 1 Discretionary Data	Consistency of Track 1 Discretionary Data (tag 9F1F) and data on the magnetic stripe T1	☐ Pass ☐ Fail ☒ Not applicable
ICC Track 2 Discretionary Data	Consistency of Track 2 Discretionary Data(tag 9F20) and Track 2 Equivalent Data (tag 57)	☐ Pass ☐ Fail ☒ Not present
ICC Track 2 Equivalent Data	Consistency of Track 2 Equivalent Data (tag 57) and data on the magnetic stripe T2	☒ Pass ☐ Fail ☐ Not applicable
TLV Encodings	Consistency of ICC data vs. defined profile and data elements format, TLV structures, duplication of data, consistency of data in the PSE and in the FCI	☒ Pass ☐ Fail
Issuer Action Codes	Validation of the Issuer Action Codes (IACs) configured for the application	☒ Pass ☐ Fail
Cardholder Verification Methods	Validation of the Cardholder Verification Methods (CVMs) supported by the application	☒ Pass ☐ Fail
Mandatory Data Elements	Presence of all mandatory data elements	☒ Pass ☐ Fail
Dynamic Data Authentication	Validation of the dynamically signed data and of the related DDA/CDA signature	☒ Pass ☐ Fail ☐ Not supported
Chip Authentication Program	Validation of the ICC settings with respect to the Chip Authentication Program (CAP) specifications	☐ Pass ☐ Fail ☒ Not supported
Dynamic Tests	Correctness of the dynamic tests that are not related to cryptography	☒ Pass ☐ Fail
Application Cryptogram Dynamic Tests[2]	Personalization of the ICC Master Keys (symmetric keys)	☐ Pass ☐ Fail ☒ Not performed
Secure Messaging Dynamic Tests[3]	Personalization of the ICC Master Keys (symmetric keys)	☐ Pass ☐ Fail ☒ Not performed
Chip CVC	Test whether the card correctly supports Chip CVC[4]	☒ Pass ☐ Fail ☐ Not supported ☐ Not performed

[2] Application Cryptogram dynamic tests are only performed on Sample Cards when the relevant test keys have been provided in the relevant CPV Service Form.

[3] Secure Messaging dynamic tests are only performed on Sample Cards when the relevant test keys have been provided in the relevant CPV Service Form.

[4] For Maestro and Cirrus cards that do not support CVC 1, test that some aspect of the discretionary data field within the magnetic stripe track are unique to the magnetic stripe and unpredictable from the data in the Track 2 Equivalent Data on the chip

Application: Mastercard Contactless (AID A0000000041010AA04)		
Test	**Test Scope**	**Test Result**
TLV Encodings	Consistency of ICC data vs. defined profile and data elements format, TLV structures, duplication of data, consistency of data in the PSE and in the FCI	☒ Pass ☐ Fail
Issuer Action Codes	Validation of the Issuer Action Codes (IACs) configured for the application	☒ Pass ☐ Fail
Cardholder Verification Methods	Validation of the Cardholder Verification Methods (CVMs) supported by the application	☒ Pass ☐ Fail
Mandatory Data Elements	Presence of all mandatory data elements	☒ Pass ☐ Fail
Dynamic Data Authentication	Validation of the dynamically signed data and of the related DDA/CDA signature	☒ Pass ☐ Fail ☐ Not supported
Dynamic CVC3 verification	Correctness of the dynamic CVC3	☐ Pass ☐ Fail ☐ Not supported ☒ Not performed
Chip Authentication Program	Validation of the ICC settings with respect to the Chip Authentication Program (CAP) specifications	☐ Pass ☐ Fail ☒ Not supported
Dynamic Tests	Correctness of the dynamic tests that are not related to cryptography	☒ Pass ☐ Fail
Application Cryptogram Dynamic Tests	Personalization of the ICC Master Key (Application Cryptogram)	☐ Pass ☐ Fail ☒ Not performed
Secure Messaging Dynamic Test	Validation if the Issuer Scripts sent to card application	☐ Pass ☐ Fail ☐ Not performed ☒ Not applicable (If contactless)

Application: Mastercard (AID A0000000041010AA01)		
Test	**Test Scope**	**Test Result**
TLV Encodings	Consistency of ICC data vs. defined profile and data elements format, TLV structures, duplication of data, consistency of data in the PSE and in the FCI	☒ Pass ☐ Fail
Issuer Action Codes	Validation of the Issuer Action Codes (IACs) configured for the application	☒ Pass ☐ Fail
Cardholder Verification Methods	Validation of the Cardholder Verification Methods (CVMs) supported by the application	☒ Pass ☐ Fail
Mandatory Data Elements	Presence of all mandatory data elements	☒ Pass ☐ Fail
Dynamic Data Authentication	Validation of the dynamically signed data and of the related DDA/CDA signature	☒ Pass ☐ Fail ☐ Not supported
Chip Authentication Program	Validation of the ICC settings with respect to the Chip Authentication Program (CAP) specifications	☐ Pass ☐ Fail ☒ Not supported
Dynamic Tests	Correctness of the dynamic tests that are not related to cryptography	☒ Pass ☐ Fail
Application Cryptogram Dynamic Tests	Personalization of the ICC Master Key (Application Cryptogram)	☐ Pass ☐ Fail ☒ Not performed
Secure Messaging Dynamic Test	Validation if the Issuer Scripts sent to card application	☐ Pass ☐ Fail ☒ Not performed ☐ Not applicable (If contactless)

Application: Mastercard (AID A0000000041010AA02)		
Test	**Test Scope**	**Test Result**
TLV Encodings	Consistency of ICC data vs. defined profile and data elements format, TLV structures, duplication of data, consistency of data in the PSE and in the FCI	☒ Pass ☐ Fail
Issuer Action Codes	Validation of the Issuer Action Codes (IACs) configured for the application	☒ Pass ☐ Fail
Cardholder Verification Methods	Validation of the Cardholder Verification Methods (CVMs) supported by the application	☒ Pass ☐ Fail
Mandatory Data Elements	Presence of all mandatory data elements	☒ Pass ☐ Fail
Dynamic Data Authentication	Validation of the dynamically signed data and of the related DDA/CDA signature	☒ Pass ☐ Fail ☐ Not supported
Chip Authentication Program	Validation of the ICC settings with respect to the Chip Authentication Program (CAP) specifications	☐ Pass ☐ Fail ☒ Not supported
Dynamic Tests	Correctness of the dynamic tests that are not related to cryptography	☒ Pass ☐ Fail
Application Cryptogram Dynamic Tests	Personalization of the ICC Master Key (Application Cryptogram)	☐ Pass ☐ Fail ☒ Not performed
Secure Messaging Dynamic Test	Validation if the Issuer Scripts sent to card application	☐ Pass ☐ Fail ☒ Not performed ☐ Not applicable

		(If contactless)

Application: Mastercard (AID A0000000041010AA03)		
Test	**Test Scope**	**Test Result**
TLV Encodings	Consistency of ICC data vs. defined profile and data elements format, TLV structures, duplication of data, consistency of data in the PSE and in the FCI	☒ Pass ☐ Fail
Issuer Action Codes	Validation of the Issuer Action Codes (IACs) configured for the application	☒ Pass ☐ Fail
Cardholder Verification Methods	Validation of the Cardholder Verification Methods (CVMs) supported by the application	☒ Pass ☐ Fail
Mandatory Data Elements	Presence of all mandatory data elements	☒ Pass ☐ Fail
Dynamic Data Authentication	Validation of the dynamically signed data and of the related DDA/CDA signature	☒ Pass ☐ Fail ☐ Not supported
Chip Authentication Program	Validation of the ICC settings with respect to the Chip Authentication Program (CAP) specifications	☐ Pass ☐ Fail ☒ Not supported
Dynamic Tests	Correctness of the dynamic tests that are not related to cryptography	☒ Pass ☐ Fail
Application Cryptogram Dynamic Tests	Personalization of the ICC Master Key (Application Cryptogram)	☐ Pass ☐ Fail ☒ Not performed
Secure Messaging Dynamic Test	Validation if the Issuer Scripts sent to card application	☐ Pass ☐ Fail ☒ Not performed ☐ Not applicable (If contactless)

ISSUE LIST

Application: Mastercard (AID A0000000041010AA04)			
ID	**Issue Reference**	**Issue Description**	**Warning or Error**
SYN_001955 EMV 451 BRAND 099	CVM list	Cards that support DDA, CDA, or both, and support offline PIN should support both offline enciphered PIN and offline plaintext PIN.	WARNING
SYN_001982 ID395	File Control Information Issuer Discretionary Data (Tag BF0C)	The tags DF40 and DF48 are present in the FCI Issuer Discretionary Data (Tag BF0C) returned in the “SELECT PSE” and “SELECT ADF” response messages. Mastercard reminds you that these tags are not in the list of BF0C expected data elements and will not be processed unless specific code is implemented in the terminal to support it. However, please note that other issuers may use the same tags for other purposes, which may lead to unpredictable results.	WARNING
SYN_002397 ID705	Log entry	The Log Entry (tag 9F4D) is present in the FCI Discretionary Data (tag BF0C) of the PSE whereas its presence is only relevant in the FCI specific to the selected ADF. An update is recommended.	WARNING
SYN_000903 ID431	Application Control	We have noticed that the card is personalized using chip grade profile whereas Mastercard recommends issuers to use semi grade profile. Semi grade profiles improve acceptance without security decrease when the Issuer Authentication Data is erroneously not delivered by the acquirer to the card. The Application Control (tag D5) Byte 1 bit 8 should be set to '1'.	WARNING
SYN_002758 ID866	Default ARPC Response Code	The Default ARPC Response Code has the value [0000] whereas the recommended value by [PDS] for chip grade Issuers is [0010] or [0014].	WARNING
SYN_002127 BRAND 208	Issuer Public Key Certificate	The Issuer Public Key length retrieved from the Issuer Public Key Certificate is shorter than Payment System Public Key length whereas [FA] recommends that : "Issuers should use an issuer key with the same length as the certifying PSPK, except when the PSPK is 1984 bits in which case issuers should use the maximum issuer key length of 1976 bits". An update is recommended.	WARNING
SYN_000460 INTER-07 001	Data Organization	The card personalization uses 12 records within 4 files. During a transaction, a [READ RECORD] command can take between 150 and 300 ms, depending on the mask used and generally a card can be personalized using 4 or 5 records, so current records organization can make a transaction longer for about 1 second. Mastercard recommends to check whether card data organization can not be optimized by reducing the number of records used in order to reduce transaction time.	WARNING

Application: Mastercard Contactless (AID A0000000041010AA04)			
ID	**Issue Reference**	**Issue Description**	**Warning or Error**
SYN_001982 ID395	File Control Information Issuer Discretionary Data (Tag BF0C)	The tags DF40 and DF48 are present in the FCI Issuer Discretionary Data (Tag BF0C) returned in the “SELECT ADF” response message. Mastercard reminds you that these tags are not in the list of BF0C expected data elements and will not be processed unless specific code is implemented in the terminal to support it. However, please note that other issuers may use the same tags for other purposes, which may lead to unpredictable results.	WARNING
SYN_002127 ID582	Issuer Public Key Certificate	The Issuer Public Key length retrieved from the Issuer Public Key Certificate is shorter than Payment System Public Key length whereas [FA] recommends that : "Issuers should use an issuer key with the same length as the certifying PSPK, except when the PSPK is 1984 bits in which case issuers should use the maximum issuer key length of 1976 bits". An update is recommended.	WARNING

Application: Mastercard (AID A0000000041010AA01)			
ID	**Issue Reference**	**Issue Description**	**Warning or Error**
SYN_001955 EMV 451 BRAND 099	CVM list	Cards that support DDA, CDA, or both, and support offline PIN should support both offline enciphered PIN and offline plaintext PIN.	WARNING
SYN_001982 ID395	File Control Information Issuer Discretionary Data (Tag BF0C)	The tags DF40 and DF48 are present in the FCI Issuer Discretionary Data (Tag BF0C) returned in the “SELECT PSE” and “SELECT ADF” response messages. Mastercard reminds you that these tags are not in the list of BF0C expected data elements and will not be processed unless specific code is implemented in the terminal to support it. However, please note that other issuers may use the same tags for other purposes, which may lead to unpredictable results.	WARNING
SYN_002397 ID705	Log entry	The Log Entry (tag 9F4D) is present in the FCI Discretionary Data (tag BF0C) of the PSE whereas its presence is only relevant in the FCI specific to the selected ADF. An update is recommended.	WARNING
SYN_000903 ID431	Application Control	We have noticed that the card is personalized using chip grade profile whereas Mastercard recommends issuers to use semi grade profile. Semi grade profiles improve acceptance without security decrease when the Issuer Authentication Data is erroneously not delivered by the acquirer to the card. The Application Control (tag D5) Byte 1 bit 8 should be set to '1'.	WARNING
SYN_002758 ID866	Default ARPC Response Code	The Default ARPC Response Code has the value [0000] whereas the recommended value by [PDS] for chip grade Issuers is [0010] or [0014].	WARNING

SYN_002127 BRAND 208	Issuer Public Key Certificate	The Issuer Public Key length retrieved from the Issuer Public Key Certificate is shorter than Payment System Public Key length whereas [FA] recommends that : "Issuers should use an issuer key with the same length as the certifying PSPK, except when the PSPK is 1984 bits in which case issuers should use the maximum issuer key length of 1976 bits". An update is recommended.	WARNING
SYN_000460 INTER-07 001	Data Organization	The card personalization uses 12 records within 4 files. During a transaction, a [READ RECORD] command can take between 150 and 300 ms, depending on the mask used and generally a card can be personalized using 4 or 5 records, so current records organization can make a transaction longer for about 1 second. Mastercard recommends to check whether card data organization can not be optimized by reducing the number of records used in order to reduce transaction time.	WARNING

Application: Mastercard (AID A0000000041010AA02)

ID	**Issue Reference**	**Issue Description**	**Warning or Error**
SYN_001955 EMV 451 BRAND 099	CVM list	Cards that support DDA, CDA, or both, and support offline PIN should support both offline enciphered PIN and offline plaintext PIN.	WARNING
SYN_001982 ID395	File Control Information Issuer Discretionary Data (Tag BF0C)	The tags DF40 and DF48 are present in the FCI Issuer Discretionary Data (Tag BF0C) returned in the “SELECT PSE” and “SELECT ADF” response messages. Mastercard reminds you that these tags are not in the list of BF0C expected data elements and will not be processed unless specific code is implemented in the terminal to support it. However, please note that other issuers may use the same tags for other purposes, which may lead to unpredictable results.	WARNING
SYN_002397 ID705	Log entry	The Log Entry (tag 9F4D) is present in the FCI Discretionary Data (tag BF0C) of the PSE whereas its presence is only relevant in the FCI specific to the selected ADF. An update is recommended.	WARNING
SYN_000903 ID431	Application Control	We have noticed that the card is personalized using chip grade profile whereas Mastercard recommends issuers to use semi grade profile. Semi grade profiles improve acceptance without security decrease when the Issuer Authentication Data is erroneously not delivered by the acquirer to the card. The Application Control (tag D5) Byte 1 bit 8 should be set to '1'.	WARNING
SYN_002758 ID866	Default ARPC Response Code	The Default ARPC Response Code has the value [0000] whereas the recommended value by [PDS] for chip grade Issuers is [0010] or [0014].	WARNING

SYN_002127 BRAND 208	Issuer Public Key Certificate	The Issuer Public Key length retrieved from the Issuer Public Key Certificate is shorter than Payment System Public Key length whereas [FA] recommends that : "Issuers should use an issuer key with the same length as the certifying PSPK, except when the PSPK is 1984 bits in which case issuers should use the maximum issuer key length of 1976 bits". An update is recommended.	WARNING
SYN_000460 INTER-07 001	Data Organization	The card personalization uses 12 records within 4 files. During a transaction, a [READ RECORD] command can take between 150 and 300 ms, depending on the mask used and generally a card can be personalized using 4 or 5 records, so current records organization can make a transaction longer for about 1 second. Mastercard recommends to check whether card data organization can not be optimized by reducing the number of records used in order to reduce transaction time.	WARNING

Application: Mastercard (AID A0000000041010AA03)			
ID	**Issue Reference**	**Issue Description**	**Warning or Error**
SYN_001955 EMV 451 BRAND 099	CVM list	Cards that support DDA, CDA, or both, and support offline PIN should support both offline enciphered PIN and offline plaintext PIN.	WARNING
SYN_001982 ID395	File Control Information Issuer Discretionary Data (Tag BF0C)	The tags DF40 and DF48 are present in the FCI Issuer Discretionary Data (Tag BF0C) returned in the “SELECT PSE” and “SELECT ADF” response messages. Mastercard reminds you that these tags are not in the list of BF0C expected data elements and will not be processed unless specific code is implemented in the terminal to support it. However, please note that other issuers may use the same tags for other purposes, which may lead to unpredictable results.	WARNING
SYN_002397 ID705	Log entry	The Log Entry (tag 9F4D) is present in the FCI Discretionary Data (tag BF0C) of the PSE whereas its presence is only relevant in the FCI specific to the selected ADF. An update is recommended.	WARNING
SYN_000903 ID431	Application Control	We have noticed that the card is personalized using chip grade profile whereas Mastercard recommends issuers to use semi grade profile. Semi grade profiles improve acceptance without security decrease when the Issuer Authentication Data is erroneously not delivered by the acquirer to the card. The Application Control (tag D5) Byte 1 bit 8 should be set to '1'.	WARNING
SYN_002758 ID866	Default ARPC Response Code	The Default ARPC Response Code has the value [0000] whereas the recommended value by [PDS] for chip grade Issuers is [0010] or [0014].	WARNING

SYN_002127 BRAND 208	Issuer Public Key Certificate	The Issuer Public Key length retrieved from the Issuer Public Key Certificate is shorter than Payment System Public Key length whereas [FA] recommends that : "Issuers should use an issuer key with the same length as the certifying PSPK, except when the PSPK is 1984 bits in which case issuers should use the maximum issuer key length of 1976 bits". An update is recommended.	WARNING
SYN_000460 INTER-07 001	Data Organization	The card personalization uses 12 records within 4 files. During a transaction, a [READ RECORD] command can take between 150 and 300 ms, depending on the mask used and generally a card can be personalized using 4 or 5 records, so current records organization can make a transaction longer for about 1 second. Mastercard recommends to check whether card data organization can not be optimized by reducing the number of records used in order to reduce transaction time.	WARNING