EMV® Interoperability Working Group

Best Practice for Biometric and Proprietary CVM Support

Version 2.0

March 2020

Legal Notice

This document summarizes EMVCo's present plans for evaluation services and related policies and is subject to change by EMVCo at any time. This document does not create any binding obligations upon EMVCo or any third party regarding the subject matter of this document, which obligations will exist, if at all, only to the extent set forth in separate written agreements executed by EMVCo or such third parties. In the absence of such a written agreement, no product provider, test laboratory or any other third party should rely on this document, and EMVCo shall not be liable for any such reliance.

No product provider, test laboratory or other third party may refer to a product, service or facility as EMVCo approved, in form or in substance, nor otherwise state or imply that EMVCo (or any agent of EMVCo) has in whole or part approved a product provider, test laboratory or other third party or its products, services, or facilities, except to the extent and subject to the terms, conditions and restrictions expressly set forth in a written agreement with EMVCo, or in an approval letter, compliance certificate or similar document issued by EMVCo. All other references to EMVCo approval are strictly prohibited by EMVCo.

Under no circumstances should EMVCo approvals, when granted, be construed to imply any endorsement or warranty regarding the security, functionality, quality, or performance of any particular product or service, and no party shall state or imply anything to the contrary. EMVCo specifically disclaims any and all representations and warranties with respect to products that have received evaluations or approvals, and to the evaluation process generally, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement. All warranties, rights and remedies relating to products and services that have undergone evaluation by EMVCo are provided solely by the parties selling or otherwise providing such products or services, and not by EMVCo, and EMVCo will have no liability whatsoever in connection with such products and services.

This document is provided "AS IS" without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in this document. 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 THIS DOCUMENT.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to this document. EMVCo undertakes no responsibility to determine whether any implementation of this document 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 this document should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, this document 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 this document 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 this document.

Contents

1 Summary

Executive Summary

EMVCo has identified a potential interoperability issue related to the acceptance of contact cards with Biometric CVM support or with a CVM that is not recognized by the terminal. It is important that the relevant issuers and entities implementing terminal kernels be alerted of this, and follow the best practices described below to prevent occurrence.

Description of the issue

EMVCo has identified that some contact kernels may behave differently with CVM Lists that include a CVM that is not recognized by the kernel when combined with the "If terminal supports the CVM" condition code ('03').

a) Some kernels bypass the CV Rule and proceed with the next CVM entry in the CVM List.
b) Some kernels examine CV Rule byte 1 bit 7 to determine subsequent processing:

0 = Fail cardholder verification if this CVM is unsuccessful

1 = Apply succeeding CV Rule if this CVM is unsuccessful

EMV Book 3 Section 10.5 states:

"If any of the following is true:

• the conditions expressed in the second byte of a CV Rule are not satisfied

…

then the terminal shall bypass the rule and proceed to the next".

The "conditions expressed in the second byte of the CV Rule", which are listed in Table 40, include "If the terminal supports the CVM"

Consequently, (a) is the correct behaviour. Specific test cases have been added to the latest test plan release (effective January 2019),

There is a potential interoperability issue since kernels approved prior to January 2019 may behave differently when encountering an unrecognized CVM. This is especially relevant given the introduction of new biometric CVMs in the *EMV Specification Bulletin No. 185 Biometric Terminal Specification*.

An Issuer that has issued cards with a CVM List having a biometric CVM entry (e.g.: '0803 0103') may expect terminals not supporting biometrics to ignore the biometric CVM and proceed with the subsequent CVM (in this example, offline PIN). A kernel incorrectly implementing the CVM List management may instead fail cardholder verification without attempting subsequent CVMs, if the unrecognized CVM is configured to fail cardholder verification when the CVM is unsuccessful.

Specifically, there are 2 possible scenarios:

- The biometric CVM entry is the last one in the CVM list: the impact should be minimum from kernels that do not recognize biometric CVM. There should be no interoperability issue as other CVMs will be performed first as is done today

- The biometric CVM precedes other recognized CVMs in the CVM List: here the kernel may fail cardholder verification due to the unrecognized biometric CVM without proceeding to the following CVM(s)

Additionally, a kernel incorrectly implementing CVM List processing may set the TVR bit “Unrecognised CVM” with cards using a biometric CVM, a payment system or an issuer proprietary Cardholder Verification Method (CVM) Codes regardless of the associated Cardholder Verification Method (CVM) Condition Code.

Impacted Market

Global

Should there be any actual interoperability issues reported from the field in the future, EMVCo will update the Interoperability Working Group Issues List.

Severity

Medium

Related Documents

None

2 Best Practice

Entity	Best Practice
Issuers	Issuers using a CVM List that includes a biometric CVM with the CVM Condition Code 'If terminal supports the CVM' should consider the following in order to enable acceptance at terminals that perform incorrect CV Rule processing: - Set CVM Code byte 1 bit 7 to '1' (Apply succeeding CV Rule if this CVM is unsuccessful) for any Biometric CVMs in the list that precede the last entry. - Not configure IACs to decline transactions where the "Unrecognised CVM" bit is set to '1'. - Consider authorization host processing for cases where TVR bit "Unrecognized CVM" is set to '1'.
Issuers	Issuers using payment system and/or issuer proprietary CVMs should also consider the above best practice.