



Update for EMV Book C-5

Change to the Processing Requirement of CDA Signature Verification failure

Applicability

This Specification Bulletin applies to:

- *EMV® Contactless Specifications for Payment Systems, Book C-5 – Kernel 5 Specification, Version 2.10, March 2021*

Related Documents

- *None*

Effective Date

- *1 January 2024*
-

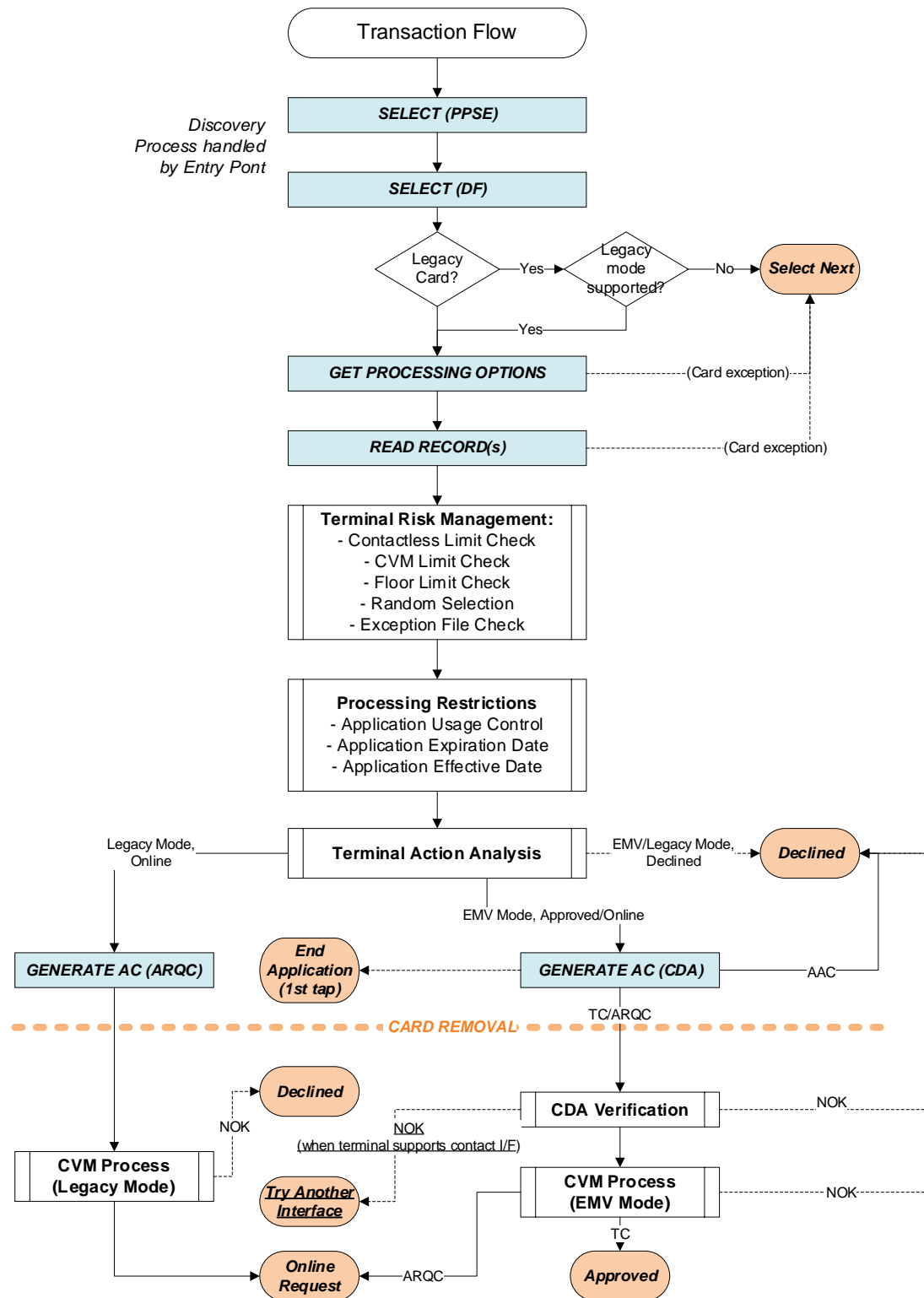
Description

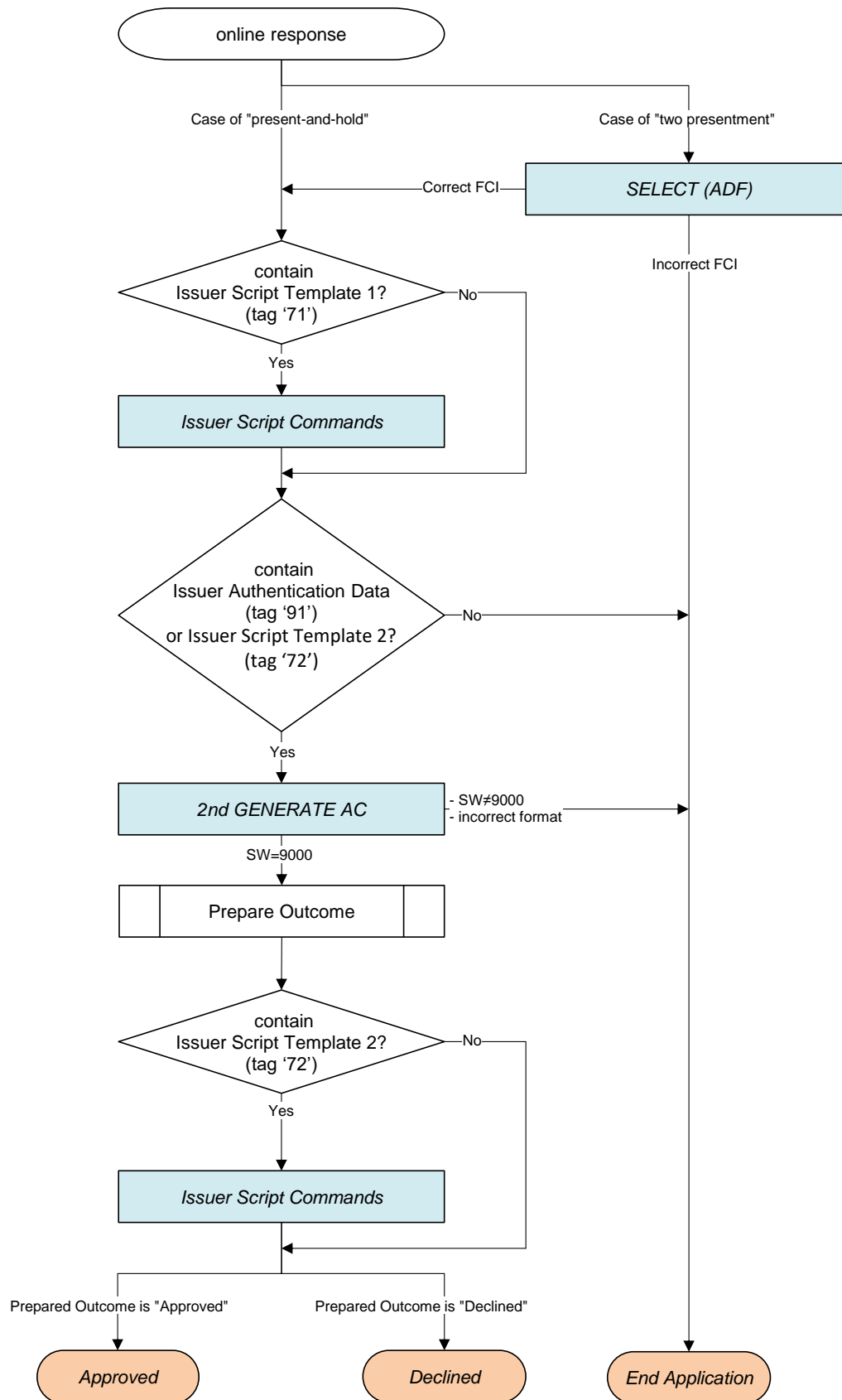
Currently, if CDA signature verification fails, the Kernel is required to terminate the transaction and provide a Decline Outcome as described in section 3.12.5. This specification bulletin changes the requirements to provide a Try Another Interface Outcome if the terminal supports the contact interface.

Also, this bulletin clarifies that TVR shall be updated in this case.

Details of Changes

(1) In section 2.3, replace Figure 2-1 with the following figure.





(2) Replace section 3.8.2.1 as follows.

Requirement – CDA Signature Verification

3.8.2.1 If the card has returned a Signed Dynamic Application Data (tag '9F4B'),
Then the Kernel shall verify the signature as defined for CDA in [EMV Book 2] and [EMV Book 3], including the retrieval of ICC Public Key.

If any step of signature verification fails,
Then

If the Terminal Interchange Profile (dynamic) indicates 'EMV contact chip supported' (byte 1 bit 2 = '1'),
Then the Kernel shall terminate the transaction with a Try Another Interface Outcome as defined in section 3.12.6.
Else the Kernel shall decline the transaction as defined in section 3.12.5.

(3) Replace footnote 6 in section 3.8.1 as follows.

The Kernel shall not change TVR after requesting GENERATE APPLICATION CRYPTOGRAM command and before providing the first Outcome, except the case of the failure of CDA Signature Verification (see 3.8.2.1).

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