EMV® Specification Bulletin No. 276
Second Edition April 2023

Clarification regarding UN in CDA signature verification

The 2nd edition of the Specification Bulletin:

- Corrects the 1st edition by moving the requirement from a footnote into the body of the text.
- Clarifies the requirement by explaining that an "An Unpredictable Number should already have been generated for the current transaction as it should have been identified in CDOL1. If not, CDA has failed.".
- Clarifies that the changes relate to v4.4 rather than v4.3 of the EMV® ICC specifications.

Applicability

This Specification Bulletin applies to

- *EMV® Integrated Circuit Card Specifications for Payment Systems, Book 2 – Security and Key Management, Version 4.4, October 2022.*

Related Documents

- *EMV Integrated Circuit Card Specifications for Payment Systems, Book 4 – Cardholder, Attendant and Acquirer Interface Requirements, Version 4.4, October 2022.*
- *EMV Specification Bulletin No.276, Clarification regarding UN in CDA signature verification, 1st edition September 2022.*

Effective Date

- *January 2024*

Description

According to Book 4, the terminal generates a 4-byte Unpredictable Number (UN, tag 9F37) to be used for input to the card cryptograms (Application Cryptograms and DDA/CDA signatures) to ensure the unpredictability of data input to this calculation and thereby the freshness of the cryptogram.

A terminal may use the same UN value throughout a transaction, or it may generate a fresh UN every time one is requested by a card DOL, however the UN value used must always be unpredictable prior to the transaction.

If an Unpredictable Number has not already been generated for the current transaction before verifying the CDA signature then CDA is considered to have failed.

To make this clear a requirement is inserted into Book 2 section 6.6.2 that describes CDA signature verification. Text inserted by the 2nd edition of this bulletin is shown in red and shown underscored. Text that had been inserted by the 1st edition of this bulletin is shown in red and shown struck through. The 2nd edition supersedes the 1st edition.

Specification Change

In Book 2 section 6.6.2 append a requirement to Step 7 as follows:

7. Concatenate from left to right the second to the sixth data elements in Table 22 (that is, Signed Data Format through Pad Pattern), followed by the Unpredictable Number.~~[30A]~~
An Unpredictable Number should already have been generated for the current transaction as it should have been identified in CDOL1. If not, CDA has failed.

~~[30A] If an Unpredictable Number has not already been generated during the transaction then the terminal shall generate an Unpredictable Number before performing this step.~~

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