Specification Bulletin No. 137
First Edition March 2014

CDA

This Specification Bulletin recommends that terminals supporting CDA support CDA in Mode 1 only. It further mandates that terminals supporting CDA check whether the terminal contains the appropriate CA Public Key before Terminal Action Analysis.

Effective Date

Recommendations in this bulletin are effective immediately. Requirements in this bulletin will be effective from November 2014, at which time any affected or new type approval testing will also come into effect.

Applicability

This Specification Bulletin applies to:

- *EMV Integrated Circuit Card Specifications for Payment Systems Version 4.3 Book 2 Security and Key Management*

Related Documents

- *None*

Description

In order to mitigate acceptance risks at terminals where the acquirer has failed to install the correct Certification Authority Public Keys, this bulletin augments the recommendation to a requirement that during CDA the terminal checks for presence of the appropriate Certification Authority Public Key before Terminal Action Analysis.[1]

In recognition of the improved performance of terminals and in order to simplify EMV kernels, this bulletin recommends that terminals supporting CDA only support Mode 1.

The recommendations identified in this bulletin are effective immediately and the requirements identified in this bulletin are applicable to devices undergoing type approval from November 2014.

Specification Change Notice

[1] Implementations of contactless specifications should however continue to follow the requirements in those specifications.

Please append the following paragraph to Section 6.2 of *EMV Book 2 Security and Key Management:*

"In the case of CDA, this step shall be performed before Terminal Action Analysis. (Refer to individual contactless kernel specifications for specific contactless requirements)."

Please append the following requirement to the end of the 3rd paragraph of Section 6.6 of *EMV Book 2 Security and Key Management:*

> "All terminals shall verify before Terminal Action Analysis that they contain the Certification Authority Public Key identified by the card. See Section 6.2. (Refer to individual contactless kernel specifications for specific contactless requirements)."

Please modify Annex D4 of *EMV Book 2 Security and Key Management* according to the changes identified on the following pages:

D4 CDA Modes

Following publication of EMV Specification Update Bulletin 44 (SU44), EMV permits flexible terminal CDA behaviour that can potentially improve transaction performance. These include the selective use of CDA for online authorisations and public key retrieval relative to Terminal Action Analysis (TAA).

CDA for online authorisations

Terminals supporting CDA have the following options:

- Request or not request CDA on ARQCs
- Request or not request CDA on 2nd GENERATE AC (TC) after an approved online authorisation

As part of the EMV type approval, a terminal kernel configuration supporting CDA must now identify which of the above options the terminal supports.

Thus an EMV terminal configuration supporting CDA will operate in one of four modes:

Mode	Request CDA on ARQC	Request CDA on 2nd GEN AC (TC) after approved online authorisation
1	Yes	Yes
2	Yes	No
3	No	No
4	No	Yes

Table 1: CDA Modes

In the years since publication of SU44 terminals have become faster, therefore the performance impact of always doing CDA, irrespective of online authorisation, is no longer significant. For this reason Mode 1 is now recommended instead of the other modes.

Public Key retrieval

Before publication of SU44, terminals experiencing CDA failure prior to TAA decline the transaction. Following publication of SU44, terminals that comply with SU44 that experience CDA failure prior to TAA shall proceed with TAA to decide whether to decline or send the transaction online.

One possible reason for CDA failing is a problem retrieving the public keys. According to SU44, terminals that find this problem before TAA will proceed with TAA to decide whether to decline or send the transaction online. Thus an online authorisation (without CDA) is possible, rather than the decline that was previously required.

SU44 also clarifies that keys can be retrieved before or after TAA which can lead to performance improvements for terminals operating predominantly online. This is because if the TAA results in an online authorisation and if the terminal requests an ARQC without CDA (i.e. it is operating in Mode 3 or 4), then the retrieval of the issuer and ICC public keys need not be completed, saving the RSA processing.[2]

Note that Section 6 now mandates for CDA that all terminals verify before TAA that they contain the Certification Authority Public Key identified by the card. Such verification does not involve time-consuming cryptographic processing. If the correct key is not present, then the Terminal Action Codes can result in Terminal Action Analysis sending the transaction online without requesting CDA in the GENERATE AC.

Recommendations

The following recommendations apply to terminals supporting CDA.

~~All terminals should verify before TAA that they contain the Certification Authority Public Key identified by the card. Such verification does not involve time-consuming cryptographic processing. If the correct key is not present, then online terminals have an opportunity to send the transaction online without requesting CDA in the GENERATE AC.~~

For online capable terminals that are able to perform certificate verification quickly, it is recommended that the terminal retrieve the issuer and ICC public keys before TAA. This is to ensure that in the unlikely event that key retrieval fails then the terminal can request an ARQC without CDA rather than decline the transaction. ~~Exceptions to this recommendation might be slower terminals which gain efficiencies by overlapping terminal certificate verification with card signature generation or Mode 3 terminals that normally send transactions online (i.e. request an ARQC rather than a TC at the first GENERATE AC) and for which a fast transaction is critical.~~

Terminal vendors are recommended to implement Mode 1 only.

As Mode 4 does not provide significant benefit, terminal vendors are recommended not to implement Mode 4. If CDA is needed on all 2nd GENERATE AC commands requesting a TC, then Mode 1 can be used.

[2] If Offline Enciphered PIN is performed then this will force the retrieval of the issuer and ICC public keys to happen before PIN verification is performed.