Specification Update Bulletin No. 64
First Edition May 2008

CPA Security Limits Status Indicators

This Specification Update Bulletin describes conditional changes to the EMV Common Payment Application (CPA) Specification for Payment Systems.

These changes clarify when the indicators that a Security Limit has been reached are to be set in Security Limits Status.

The changes in this bulletin will be incorporated into version 1.0.d of the CPA Card Type Approval documentation (that is, Test Cases, Card Images, and Implementation Conformance Statement).

This bulletin is optional for all CPA cards that implement the Application Security Counters implementer-option as described in CPA annex F, effective 1 November 2008.

This bulletin is conditional for all CPA cards that implement the Application Security Counters implementer-option as described in CPA annex F, effective 1 November 2009.

Applicability

This Specification Update Bulletin applies to:

- *EMV Common Payment Application Specification Version 1.0 December 2005*

Related Documents

- Specification Update bulletin 56 – CPA Corrections and Changes
- The CPA card approval test cases will be modified in accordance with the final Specification Update bulletin.

Description

This Specification Update Bulletin describes changes to the *EMV Common Payment Application Specification*. These changes clarify when the indicators that a Security Limit has been reached are to be set in Security Limits Status.

The CPA data element Security Limits Status has bits that are set when the AC (Application Cryptogram) Session Key Counter reaches its limit, the SMI (Secure Messaging for Integrity) Session Key Counter reaches its limit, and the PIN Decipherments Error Counter reaches its limit. Annex F (which describes one way to implement the Security Counters implementer-option in CPA) describes the incrementing of the associated counters, but does not describe when the bits in Security Limits Status are to be set. This bulletin clarifies when the bits are set.

Specification Change Notice

Please make the following changes to *EMV Common Payment Application Version 1.0*.

In CPA Annex F1 (as updated by Edit 3 from SU 56), page F-1, insert the text ", the 'AC Session Key Counter Limit Exceeded' bit in Security Limits Status is set to the value 1b," as shown underscored in the following:

> "Initiation of AC session key derivation is controlled as follows:
>
> 1. If the AC Session Key Counter has reached the AC Session Key Counter Limit (that is, if Counter ≥ Limit), then session key derivation is aborted, the 'AC Session Key Counter Limit Exceeded' bit in Security Limits Status is set to the value 1b, and the application responds to the Generate AC command with SW1 SW2 = '6985'.
> 2. If the AC Session Key Counter has not reached the AC Session Key Counter Limit, the Counter is incremented and saved in non-volatile memory. The application continues with the AC session key derivation process.
>
> The AC Session Key Counter is reset to zero only when an ARPC is successfully validated.
>
> The AC Session Key Counter Limit shall be less than or equal to 'FF FF'.

In CPA Annex F1 (as updated by Edit 3 from SU 56), page F-2, insert the text ", the 'SMI Session Key Counter Limit Exceeded' bit in Security Limits Status is set to the value 1b," as shown underscored in the following:

> "SMI session key derivation is only performed if the card receives a script command. Initiation of the SMI session key derivation is controlled as follows:
>
> 1. If the SMI Session Key Counter has reached the SMI Session Key Counter Limit (that is, if Counter ≥ Limit), then session key derivation is aborted, the 'SMI Session Key Counter Limit Exceeded' bit in Security Limits Status is set to the value 1b, and the application responds to the script command with SW1 SW2 = '6985'.
> 2. If the SMI Session Key Counter has not reached the SMI Session Key Counter Limit, the Counter is incremented and saved in non-volatile memory. The application continues with the SMI session key derivation process.
>
> The SMI Session Key Counter is decremented if the first MAC in the script is successfully validated.
>
> The SMI Session Key Counter Limit shall be less than or equal to 'FF FF'."

In CPA Annex F2, page F-3, replace the first two bullets with the following:

"

- If the PIN Decipherments Error Counter has reached the PIN Decipherments Error Counter Limit (that is, if Counter ≥ Limit), the 'PIN Decipherments Error Counter Limit Exceeded' bit in Security Limits Status is set to the value 1b, and the application discontinues processing the VERIFY command and responds with SW1 SW2 = '6984' (Command not allowed; referenced data invalidated).

- If the PIN Decipherments Error Counter has not reached the PIN Decipherments Error Counter Limit, the-PIN Decipherments Error Counter is incremented by one and saved in non-volatile memory whilst processing the VERIFY command for the purposes of verifying an enciphered PIN and prior to accessing the PIN decipherment private key.

"