CPACE DIC Technical Note

Card "mute" functionality

This Technical Note applies to CPACE Dual Interface Card certification testing.

1.1 Introduction

Requirement Req C.13 of the *"CPACE for Dual Interface Cards Functional Specifications"* mentions that "If, by means of this mechanism, contactless access to the CPACE card is deactivated, the contactless interface of the CPACE card shall be **mute** on the attempt to start a card session."

With this document, the ECPC Technical Working Group wants to provide more information on this requirement, and on what is expected from CPACE implementations with regard to this requirement.

1.2 Rationale behind the "Mute" requirement

The main reason for the "Mute" requirement is security related.

- In post personalization, during the card distribution phase, deactivating/muting the card makes the detection of the card in a stack of letters less easy.
- For cardholder fearing fraud leveraging on the contactless interface, at least the EMV application should not be selectable. In this context, a full (and permanent) deactivation of the RF macrocell is the best solution.

1.3 Possible implementation

To implement the "mute" functionality, a distinction can be made between four types of grades. The States and Commands referred to below, map with the definition used in Chapter 7 (for Type A) and Chapter 8 (for Type B) of the *"EMV® Level 1 Specifications for Payment Systems – EMV Contactless Interface Specification – Version 3.0 – February 2018"*.

- **Grade A:** RF silent card
  - The RF macrocell on the chip is disabled by the card OS during the boot.
  - In this case, the card will get power from the antenna, the card OS will boot, but the RF macrocell will not retromodulate at all over RF.
  - The reader will send REQA/REQB, but the card does not reach the READY State.
- **Grade B:** RF capable card, but mute (at application level)
  - The RF macrocell is active.
  - The card responds to the reader's commands but only until a READY State is reached.

  - The card does not respond to any (protocol level) SELECT (CLx) command. This means the ACTIVE State is not reached.
  - The card does not send an ATS. Therefore, no C-APDUs should be sent to the card.

- **Grade C:** RF capable card, but mute (at application level)
  - The RF macrocell is active, but the OS does not accept any APDU commands.
  - In this case, the card will retromodulate, and will probably successfully pass the anticollision phase. An ATS will be seen on the reader, built from the anticollision data.
  - The protocol is established. The reader may send C-APDU, but no R-APDU answer will be sent back by the card.
  - Selection of the applications (PPSE and EMV) will therefore not work.
- **Grade D**: RF capable card, unmuted, with unselectable EMV applications
  - The RF macrocell is active, anticollision phase works, and the OS accepts APDU commands. The PPSE can be selected but EMV applications cannot not be selected.
  - The protocol is established.
  - In this case, the C-CAPUs will be answered to. Some SELECT commands will succeed (i.e response with SW1 SW2 = '9000', for example to SELECT PPSE) while others will fail (i.e. SW1 SW2 <> '9000', for example in case of EMV applications).

1.4 Acceptable implementations

- Grade A is the recommended implementation.
- Grade B and Grade C:
  - For Type A cards, is acceptable
  - For Type B cards, depends on the way the PUPI (Pseudo-unique PICC Identifier) is implemented. The PUPI is an identifier used at protocol level, that can either be a random value (that is re-generated at each anticollision cycle) or a fixed value.
    - If the PUPI is random, the Grade B or C implementation is acceptable.
    - If the PUPI is a fixed value (e.g. configured as such in the card OS), it must be possible to deactivate the RF macrocell to avoid that the card reveals its fixed PUPI. In this case the Grade B or C implementation is not acceptable. Note that if the business context justifies it, a waiver could be granted for specific markets.
- Grade D is not acceptable.

1.5 Testing

From the above description of the possible implementations of the "mute" functionality, it is clear that depending on the Grade, the muting is done on the protocol or on the functional level. This also means that from a testing perspective, we are looking at this boundary, which reflects in the test equipment that is required to distinguish between the different grades.
CPACE functional specification testing assumes that the EMV Contactless Protocol is correctly established. Therefore, the test equipment for CPACE functional testing uses a standard PC/SC

reader. This test equipment allows making a distinction between Grade A, B and C on the one hand and Grade D on the other hand.
With the standard functional test tool, Grade D behaviour can easily be tested. After receiving the SELECT PPSE, the card must not send a response. The test tool shall therefore wait fo a given interval. If in this interval, a response is received from the card (which is the case for a Grade D card), the test shall fail.

To further distinguish between Grade A, B and C, a protocol analyser would be required. When using the protocol analyser, one can verify that:

- In a Grade C implementation, the card does not send I-blocks containing the R-APDU data
- In a Grade B implementation, the card does not send an ATS
- In a Grade A implementation, the card does not respond to the REQA/REQB

The protocol analyser must be used in case of Type B cards, to verify if the PUPI is random, since Grade B or C implementations are not acceptable with fixed PUPI.