

**Requirements
for an EMVCo
Common Contactless Application (CCA)**

20.01.2009

CIR Technical Working Group

Table of Contents

1	Introduction	1
2	Common Contactless Application Business Requirements.....	2
3	Card Requirements	3
4	Terminal Requirements	4
4.1	General Requirements	4
4.2	Terminal Application Transaction Flow	4
4.2.1	Transaction Flow Overview	4
4.2.2	Application Selection – Entry Point Specification	5
4.2.3	Initiate Application Processing	5
4.2.4	Read Application Data	5
4.2.5	Offline Data Authentication	5
4.2.6	Processing Restrictions.....	6
4.2.7	Cardholder Verification.....	6
4.2.8	Terminal Risk Management	6
4.2.9	Terminal Action Analysis.....	7
4.2.10	Card Action Analysis	7
4.2.11	Online Processing	7
4.2.12	Issuer-To-Card Script Processing	7
4.2.13	Completion	7
5	References.....	7

1 Introduction

On behalf of the European EMV Users Group, the CIR Technical Working Group has developed Business Requirements for a Common Contactless Application (see section 2 of this document), which have been presented during EMVCo Board of Advisors Meeting in June 2008.

The European EMV Users and the CIR Technical Working Group want to come as soon as possible to the specification of a Common Contactless Application which complies with these Business Requirements. Therefore, and in order to support EMVCo in the review of their policy on contactless specifications, the CIR Technical Working Group - on behalf of the European EMV Users - has progressed with the development of the Common Contactless Application specification by identifying the Card Requirements and the Terminal Requirements for an EMVCo Common Contactless Application. These are submitted to EMVCo via the EMVCo Board of Advisors as an input for the development of an EMVCo specification for a Common Contactless Application.

The Card Requirements (see section 3 of this document) take into account that the Common Contactless Card Application shall be based on the Common Payment Application Specification (CPA) with the aim to make only minimal changes to CPA if possible. The main reasons for this relate to the following aspects:

- Issuers considering the implementation of CPA would like to see a contactless enhancement to CPA so that they are able to offer both contact-based and contactless payments using the same platform. Otherwise they would be forced to stick to scheme-specific platforms at least for contactless payments. Especially for those issuers who have not invested yet into a major roll-out of contactless payments, it would be just in time to start the development of a CPA-based Common Contactless Application.
- The longer the development of a Common Contactless Application is delayed the more difficult a future convergence of the currently diverging specifications will become, since the number of terminals which will have to be upgraded to support also a Common Contactless Application, will increase significantly. Therefore, also from the point of card acceptance, it becomes desirable to start the development of a Common Contactless Application as soon as possible.
- Especially for those issuers and acquirers who are currently investing only in pilots it would be of major benefit to have a Common Contactless Application available if it comes to a larger roll-out.

The Terminal Requirements (see section 4 of this document) define the outlines of a Common Contactless Terminal Application that supports at least the Common Contactless Card Application. The basis for this outline is the standard EMV application and transaction flow for contact chip cards as in [EMV Book 3]. Changes to this process are minimized. The necessary changes identified so far are:

- For contactless cards the Offline CAM, when performed, is CDA.
- The process steps that involve card interactions are performed in one sequence; the evaluation of the responses is performed after the end of the card interaction, when possible.
- There is no card interaction after the online process. The Issuer Scripting and the Completion process (2nd Generate AC) are not performed. The card isn't supposed to stay in the active field during the online process.

The Terminal Requirements consider only the one-Tap fast contactless process. This does not preclude other contactless processing modes, e.g. a full-EMV contactless processing mode, with and without PIN entry, either with the card that remains for a longer time in the field, or with a 2-Tap process. These considerations are out of scope of this description.

2 Common Contactless Application Business Requirements

The following Business Requirements for a Common Contactless Application identified by the CIR Technical Working Group have been presented during EMVCo Board of Advisors Meeting in June 2008:

1. Define a common infrastructure for contactless payment supporting any payment brand
2. The specification of the common infrastructure should be available as soon as possible
3. For the time being it is acceptable to have a solution limited to the ID-1 form factor. Do not wait for maturity of additional form factors, but accept that changes of CCA may be needed if and when other form factors are to be integrated
4. Shall meet the current EMVCo transaction time requirements of at most 500 ms for payment (card present time, including card and terminal processing and transmission time)
5. Shall provide a consistent user experience
6. Shall minimise changes for the back office systems

7. The card application should maximise the reuse of CPA functionality possibly limited by other business requirements (like transaction time, complexity)
8. The card application shall be able to work in combination with CPA on the contact side
9. Changes to CPA because of contactless extensions are acceptable for the card application but such changes shall be described as implementer options within the existing CPA specification
10. If the card application will be part of the CPA specification it shall be specified as an implementer option in the CPA specification
11. The card application shall minimise costs for testing and approval for dual issuance environments
12. The card application need not be backward compatible with legacy contactless terminal kernels
13. The terminal kernel should maximise the reuse of EMV contact functionality possibly limited by other business requirements like transaction time. Note: this does not mean it is required to integrate contactless and contact terminal kernels
14. The terminal kernel shall be compliant with the EMV Entry Point Specification [EMV Entry Point]
15. Conduct and provide the results of a security risk analysis for the common contactless infrastructure. The risk analysis could have impacts on specification and lead to the identification of new security requirements and development of new mechanisms

3 Card Requirements

Cards with the Common Contactless Card Application shall support the contactless transmission mode according to the EMV Contactless Communication Protocol Specification [EMV Protocol].

For CPA compliant cards the only requirements additional to CPA to support the Common Contactless Card Application are:

- The current transmission mode shall be used in Profile Selection based on the CPA Implementer Option "Profile Selection Using Card Data".

This is due to the fact that different profiles for contactless and contact based transactions are needed (e.g. different AFL, CVM-List, etc.).

- CDA shall be supported for offline processing.

4 Terminal Requirements

4.1 General Requirements

Terminals with the Common Contactless Terminal Application shall support the contactless transmission mode according to the EMV Contactless Communication Protocol Specification [EMV Protocol].

The Common Contactless Terminal Application shall meet the following general requirements:

- The application shall support and comply with the EMV Entry Point Specification.

Therefore this application is based on an implementation of the EMV Entry Point Specification.

- The application shall support at least the CVM Method "No CVM Required". If PIN is required, it is Online PIN.
- The terminal application shall complete all card interactions in less than 500 msec, which is the total time that the card resides in the active field, including card and terminal processing and transmission time.

4.2 Terminal Application Transaction Flow

This outline refers to the EMV contact Transaction Flow as described in [EMV Book 3] and presents the differences with regard to this specification.

4.2.1 Transaction Flow Overview

[EMV Book 3], Section 8.2 gives an example transaction flowchart. A new example transaction flowchart may be necessary for the Common Contactless Terminal Application specification.

4.2.2 Application Selection – Entry Point Specification

Application Selection shall be performed as described in the Entry Point Specification.

The Entry Point Pre-Processing shall be performed as described in section 5.2.2 of the EMV Entry Point Specification up to and including requirement 5.2.2.10.

Kernel Selection:

The support of the Common Contactless Terminal Application is indicated (by the card) with Byte 1 bit 8 in the Contactless Application Capabilities Type, this is "EMV Contactless Application present".

4.2.3 Initiate Application Processing

Initiate Application Processing shall be performed as described in [EMV Book 3], Section 10.1

Note: Card applications may need to make a distinction between different processing modes of the Common Contactless Terminal Application (e.g. a full EMV mode); this can be performed by a data element provided in the GPO command.

4.2.4 Read Application Data

Read Application Data shall be performed as described in [EMV Book 3], Section 10.2

This includes the checking of the presence of mandatory and conditional data elements following section 7.2 (mandatory data elements, action abort) and section 7.5 (presence of data elements, action setting a bit in TVR) of [EMV Book 3].

4.2.5 Offline Data Authentication

Offline Data Authentication shall be performed as described in [EMV Book 3], Section 10.3, with the exception of the sequence of execution.

- An Online Only contactless terminal may choose to not support offline authentication at all.
- An offline capable contactless terminal shall support only CDA as offline data authentication (ODA) method (no SDA, no DDA).

- The complete CDA process, including the retrieval and validation of the Issuer and the ICC Public Key, may optionally be delayed until after the contactless card leaves the active field.
- If the CDA process fails, then this will be detected after the contactless card leaves the active field. The transaction will be declined.

4.2.6 Processing Restrictions

Processing Restrictions shall be performed as described in [EMV Book 3], Section 10.4.

4.2.7 Cardholder Verification

If the "Terminal CVM Required Limit Exceeded"-flag is not set, then the cardholder verification process is skipped.

If "Terminal CVM Required Limit Exceeded"-flag is set, then the cardholder verification process shall be performed as described in [EMV Book 3], Section 10.5 with the following changes:

- The CVM-List process is performed.
- If the chosen method is Online PIN, then the PIN entry process will be delayed until after card interaction, but the Online PIN performed bit of the TVR will be set.
- Offline PIN and signature CVM processing shall not be supported

4.2.8 Terminal Risk Management

Terminal Risk Management shall be performed as described in [EMV Book 3], Section 10.6. with the following exceptions:

- If Floor Limit Checking is performed, then the process will not check the transaction log for log entries with the same PAN (split sales).
- Random Transaction Selection is not performed
- Velocity checking is not performed.
- If exception file checking is supported, then it shall be performed after the contactless card leaves the active field.

4.2.9 Terminal Action Analysis

Terminal Action Analysis shall be performed as described in [EMV Book 3], Section 10.7.

4.2.10 Card Action Analysis

Card Action Analysis shall be performed as described in [EMV Book 3], Section 10.8.

At the end of this step, the card can be removed from the active field.

If CDA was requested then the CDA process is performed at this point. The decision to either approve, go online or decline is taken after the CDA process is completed.

4.2.11 Online Processing

Online Processing shall be performed as described in [EMV Book 3], Section 10.9.

4.2.12 Issuer-To-Card Script Processing

Issuer-To-Card Script Processing is not performed.

4.2.13 Completion

Completion is not performed.

5 References

- | | |
|-------------------|--|
| [CPA] | EMV Integrated Circuit Card Specifications for Payment Systems, Common Payment Application Specification, Version 1.0, December 2005 |
| [EMV Book 3] | EMV Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification, Version 4.2, June 2008 |
| [EMV Entry Point] | EMV Contactless Specifications for Payment Systems, Entry Point Specification, Version 1.0, May 2008 |

[EMV Protocol] EMV Contactless Specifications for Payment Systems, EMV Contactless Communication Protocol Specification, Version 2.0, August 2007