Common Payment Application
Contactless Extension

CPACE

Functional Specification

CPACE for Dual Interface Cards

Version 1.0

18.10.2017

Notice

This Specification has been prepared by Bancomat, Bancontact Company, BankAxept, Borica, Euro 6000, girocard/SRC, Groupement des Cartes Bancaires CB, ServiRed, SIBS MB and Sistema 4B (hereinafter referred to as Cooperation) who are joint owners of the copyright therein. Permission is hereby granted to use the document solely for the purpose of implementing the Specification subject to the following conditions: (i) that none of the participants of the Cooperation nor any contributor to the Specification shall have any responsibility or liability whatsoever to any other party from the use or publication of the Specification; (ii) that one cannot rely on the accuracy or finality of the Specification; and (iii) that the willingness of the participants of the Cooperation to provide the Specification does not in any way convey or imply any responsibility for any product or service developed in accordance with the Specification and the participants of the Cooperation as well as the contributors to the Specification specifically disclaim any such responsibility to any party.

Implementation of certain elements of this Specification may require licenses under third party intellectual property rights, including without limitation, patent rights. The Participants of the Cooperation and any other contributors to the Specification are not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights. **This Specification is provided "AS IS", "WHERE IS" and "WITH ALL FAULTS", and no participant in the Cooperation makes any warranty of any kind, express or implied, including any implied warranties of merchantability, non-infringement of third party intellectual property rights (whether or not the Participants of the Cooperation have been advised, have reason to know, or are otherwise in fact aware of any information), and fitness for a particular purpose (including any errors and omissions in the Specification).**

To the extent permitted by applicable law, neither the Participants of the Cooperation nor any contributor to the Specification shall be liable to any user of the Specification for any damages (other than direct actual out-of-pocket damages) under any theory of law, including, without limitation, any special, consequential, incidental, or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, nor any damages arising out of third party claims (including claims of intellectual property infringement) arising out of the use of or inability to use the Specification, even if advised of the possibility of such damages.

The Specification, including technical data, may be subject to export or import regulations in different countries. Any user of the Specification agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import the Specification.

Revision History

Version	Date	Author	Object
Draft 1.0	04.07.2016	ECPC	First draft covering CPACE-DIC
	07.12.2016	ECPC	Second draft covering CPACE-DIC
	29.03.2017	ECPC	Changes according to vendor comments
	18.10.2017	ECPC	Integration of Relay Resistance Protocol

Table of Contents

Tables

Requirements

1 Introduction

The EMVCo Common Payment Application Specification ([CPA]) has been designed to support contact transactions only. According to this specification, an extension of [CPA] defining the data elements and functionality of an application also supporting contactless transactions for contactless cards, is called a **Common Payment Application Contactless Extension** (CPACE) specification.

As in [EMV A], according to this specification, a contactless card is considered to be a consumer device into which integrated circuit(s) and coupling means have been placed and in which communication to such integrated circuit(s) is done by inductive coupling in proximity of a coupling device. The consumer device may be a chip card of the ID 1 form factor (as defined in [ISO 7810]), a contactless only chip card, a sticker, a key fob, a mobile phone, or another form factor.

Irrespective of the form factor, according to this specification, a contactless card shall support the contactless interface according to [EMV D].

According to this specification, if not stated otherwise, the term "card" refers to a contactless card. An implementation of the functionality defined by a CPACE specification is called a **CPACE implementation**. The term "**CPACE card**" refers to a card with a CPACE implementation.

Depending on the respective environment, i.e. the form factor of the CPACE card and the CPACE card's component hosting the CPACE implementation, the following **CPACE variants** are distinguished:

Environment	**CPACE Variant**
Dual interface card (ID 1 format according to [ISO 7810])	CPACE for Dual Interface Card (CPACE-DIC)
Contactless only consumer device without a cardholder interface (e.g. a contactless only chip card in ID 1-Format or in another format, a sticker, a key fob)	CPACE for Contactless Only Device (CPACE-CLC)
Host Card Emulation (HCE) in a consumer device (e.g. a mobile phone)	CPACE for HCE in Consumer Device (CPACE-HCE)
Secure Element (SE) in a consumer device (e.g. a mobile phone)	CPACE for SE in Consumer Device (CPACE-SE)

This specification covers CPACE for Dual Interface Card (CPACE-DIC).

In particular, in this specification, the term "card" refers to a dual interface card in ID 1 format according to [ISO 7810].

When the functionality of an application complying with this specification is described in general, the application is referred to as "**the** CPACE application. But "**a** CPACE application" or "an instance of the CPACE application" refers to a program and associated data which are an implementation of this specification on a card.

In the same way as [CPA] describes the functionality of the CPA application for contact transaction (see Section 6.2 of [CPA]), this specification describes the functionality of the CPACE application for contact and contactless transactions as a state machine, where state transitions are caused by commands as defined in [CPA] or as defined in this specification: As a result of the CPACE application receiving and processing a command, the state may change before the application accepts the next command. Being an extension of [CPA], this specification has to be read in conjunction with [CPA].

All requirements and associated flow diagrams concerning the card application specified in [CPA] also apply for the CPACE application **irrespective of the interface in use**, unless stated otherwise in this specification.

Part II and Part III of [CPA] contain the following information:

1. Specification of card and application requirements, defining the card behaviour that shall be implemented by card vendors,
2. Explanation about EMV contact transactions, including terminal behaviour.

The explanation about EMV contact transaction processing, including terminal behaviour, given in [CPA] also applies for contact transaction processing with the CPACE application.

According to this specification, EMV contactless transaction processing and terminal behaviour are expected to comply with [EMV A] and [EMV B] with kernel processing analogous to EMV contact transaction processing, but including a Relay Resistance Protocol as implementer option. The following Figure 1 shows contactless transaction processing supported by the CPACE application.

Like EMV contact transaction processing, contactless transaction processing with the CPACE application is driven by the terminal. After establishing the contactless communication protocol, terminal and CPACE card communicate over the contactless interface through commands sent from the terminal to the card, and responses received by the terminal from the card.

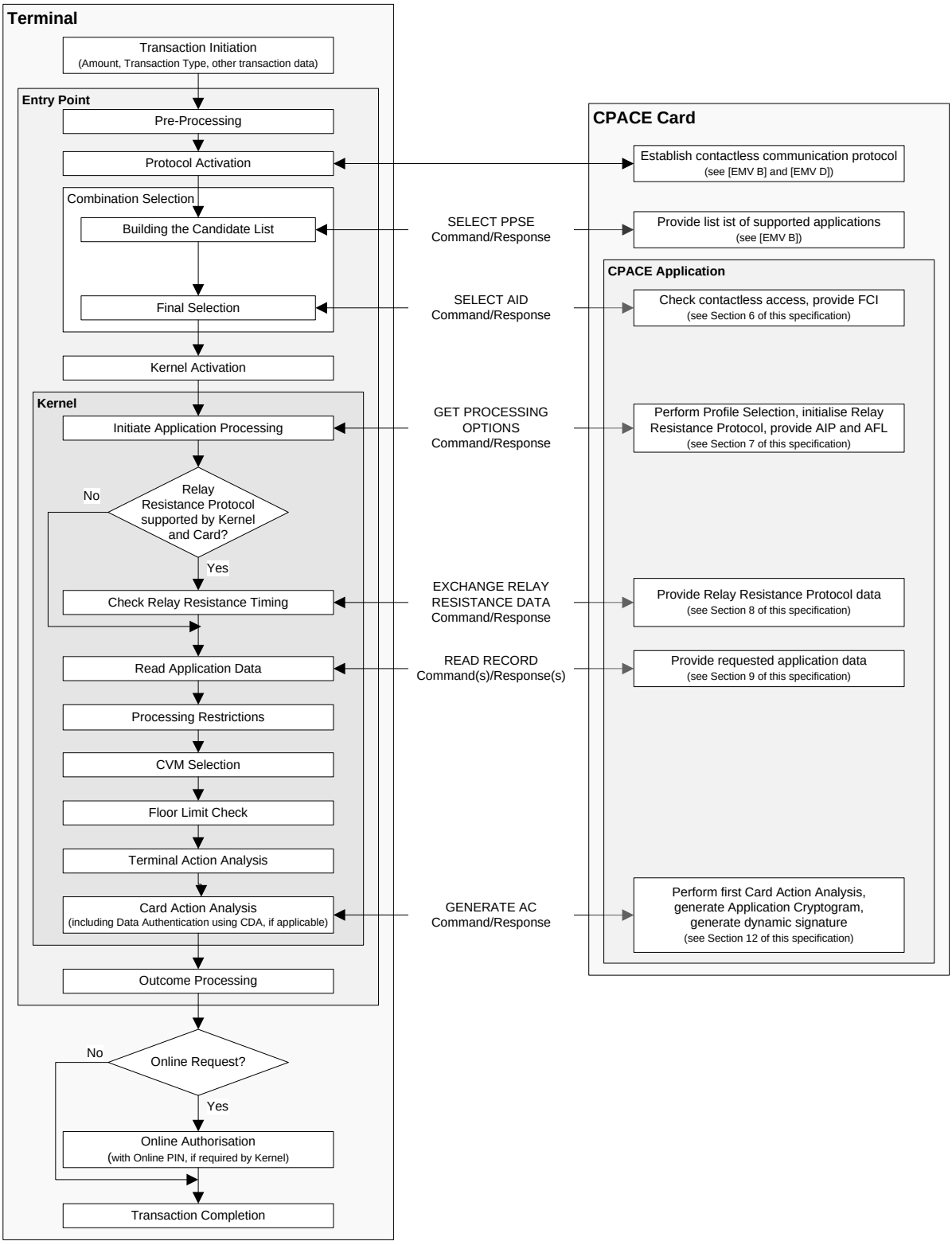

Figure 1: Contactless Transaction Flow

The main structure of this specification follows that of [CPA]. The following Table 1 maps the main sections of [CPA] to sections of this specification.

Sections of [CPA] which have a counterpart in this specification according to Table 1 are modified according to this specification.

Note:

The function flow charts in the modified sections of [CPA] have not been adapted according to the modified or new requirements in this specification.

Sections 3 and 8 of this specification do not have a counterpart in [CPA]. Section 3 of this specification adds general requirements to [CPA]. Section 8 of this specification contains the requirements for processing the EXCHANGE RELAY RESISTANCE DATA command during contactless transactions which is not part of [CPA].

Section of [CPA]		**Section of this Specification**	
1	Scope	-	-
2	Normative References	2.1	References
3	Definitions	2.2	Definitions
4	Abbreviations, Notations, Conventions, Terminology, and Symbols	2.3	Abbreviations
		2.4.1	Notation
		2.4.2	Requirement Notation
5	Overview	4	Overview and Additional Functionality
6	General Command Information	5	General Command Information
7	Application Selection	6	Application Selection
8	Initiate Application Processing	7	Initiate Application Processing
9	Read Application Data	9	Read Application Data
10	Offline Data Authentication	10	Offline Data Authentication
11	Processing Restrictions	-	-
12	Cardholder Verification	11	Cardholder Verification
13	Terminal Risk Management	-	-
14	Terminal Action Analysis	-	-
15	First Card Action Analysis	12	First Card Action Analysis
16	Online Processing	-	-
17	Second Card Action Analysis	13	Second Card Action Analysis
18	Issuer Script Command Processing	14	Issuer Script Command Processing
19	Additional Functions	4	Overview and Additional Functionality
20	Security and Key Management	15	Security and Key Management
21	Personalisation	16	Personalisation
Annex A	Profile Selection File Processing	-	-
Annex B	Additional Check Table Functionality	-	-

Section of [CPA]		Section of this Specification	
Annex C	Currency Conversion Functionality	-	-
Annex D	Transaction Logging	17	Transaction Logging
Annex E	Management of Dates in Days	-	-
Annex F	Security Counters	18	Security Counters
Annex G	Management of Profile Data	-	-
Annex H	Issuer Profile Options Specification and Processing	-	-
Annex I	Understanding Cyclic Accumulators	-	-
Annex J	GET DATA and PUT DATA Data Elements	19	GET DATA and PUT DATA Data Elements
Annex K	Data Element Tags	20	Data Elements Tags
Annex L	Data Dictionary	21	Data Dictionary

Table 1: Sections of [CPA] Modified by This Specification

2 References, Abbreviations and Document Conventions

2.1 References

[CPA] EMV Integrated Circuit Card Specifications for Payment Systems, Common Payment Application Specification, Version 1.0, December 2005

Specification Bulletin 165: AES in CPA (Spec change), 1st Edition, May 2015

Specification Bulletin 162: AES Key Derivation Erratum (Spec Change), 1st Edition, April 2015

Specification Bulletin 145: Clarification on the Format of ICC Public Key Exponent (Spec Change), 1st Edition, September 2014

Specification Bulletin 139: Clarification on Data Content for DGIs '3Fxx' (Spec Change), 1st Edition, March 2014

Specification Bulletin 90: CPA Select Response for Blocked Applications (Spec Change), 1st Edition, September 2011

Specification Bulletin 84: CPA Specification Update (Spec Change), 1st Edition, December 2010

Specification Bulletin 81: CPA Currency Conversion Accumulator Overflow (Spec Change), 1st Edition, February 2010

Specification Update Bulletin 65: CPA Last Online Transaction Not Completed (Spec Change), 1st Edition, May 2008

Specification Update Bulletin 64: CPA Security Limits Status Indicators (Spec Change), 1st Edition, May 2008

Specification Update Bulletin 63: CPA Update of VLP Available Funds (Spec Change), 3rd Edition, May 2008

Specification Update Bulletin 62: CPA Personalisation of Log Entry with EMV-CPS (Spec Change), 2nd Edition, May 2008

Specification Update Bulletin 58: Editorial Errors in Release 1.0 of the CPA Specification (Spec Change), 4th Edition, May 2008

Specification Update Bulletin 60: CPA Logging Data Element Minimums (Spec Change), 2nd Edition, February 2008

Application Note 40: CPA Personalisation of Duplicate Record Data (Clarification), 1st Edition, February 2008

Application Note 39: CPA Transaction Logging Controls in Application Control (Clarification), 1st Edition, February 2008

Specification Update Bulletin 61: CPA Additional Check Table Error Processing (Spec Change), 1st Edition, August 2007

	Specification Update Bulletin 56: CPA Corrections and Changes (Spec Change), 2nd Edition, February 2007
[CPS]	EMV Card Personalization Specification, Version 1.1, July 2007
[EMV 1]	EMV Integrated Circuit Card Specifications for Payment Systems, Book 1, Application Independent ICC to Terminal Interface Requirements, Version 4.3, November 2011
[EMV 2]	EMV Integrated Circuit Card Specifications for Payment Systems, Book 2, Security and Key Management, Version 4.3, November 2011
[EMV 3]	EMV Integrated Circuit Card Specifications for Payment Systems, Book 3, Application Specification, Version 4.3, November 2011
[EMV A]	EMV Contactless Specifications for Payment Systems - Book A - Architecture and general requirements, Version 2.6, March 2016
[EMV B]	EMV Contactless Specifications for Payment Systems - Book B - Entry Point Specification, Version 2.6, July 2016
[EMV D]	EMV Contactless Specifications for Payment Systems, Book D, EMV Contactless Communication Protocol Specification, Version 2.6, March 2016
[EMV SB175]	EMV Specification Bulletin No. 175, Application Selection Registered Proprietary Data, First Edition, February 2016
[ISO 3166-1]	Codes for the representation of names of countries and their subdivisions – Part 1: Country codes
[ISO 7810]	ISO/IEC 7810, Identification cards – Physical characteristics

2.2 Definitions

In addition to those provided in Section 3 of [CPA], the definition listed below is used in this specification.

Card Session	The link between the card and the external world starting at card reset (contact cards), activation (contactless cards), or power on of the card and ending with a subsequent reset (contact cards), deactivation (contactless cards), or power off of the card.

2.3 Abbreviations

In addition to those listed in Section 4.1 of [CPA], the abbreviations listed below are used in this specification.

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit

CPACE	Common Payment Application Contactless Extension
CPACE-DIC	Common Payment Application Contactless Extension for Dual Interface Card
CPACE-CLC	Common Payment Application Contactless Extension for Contactless Only Device
CPACE-SE	Common Payment Application Contactless Extension for SE in Consumer Device
CPACE-HCE	Common Payment Application Contactless Extension for HCE in Consumer Device
DGI	Data Grouping Identifier
ERRD	EXCHANGE RELAY RESISTANCE DATA
HCE	Host Card Emulation
IDD	Issuer Discretionary Data
ILDOL	Internal Log Data Object List
PAD	Proprietary Authentication Data
PPSE	Proximity Payment System Environment
PSE	Payment System Environment
R-APDU	Response APDU
RRP	Relay Resistance Protocol
SDAD	Signed Dynamic Application Data
SE	Secure Element
SK_{AC}	Application Cryptogram Session Key

2.4 Document Conventions

This specification uses the data element format conventions, terminology and flowchart symbols defined in Sections 4.3, 4.4 and 4.6 of [CPA]. This specification uses the notation defined in Section 4.2 of [CPA], with the additions and modifications described in Section 2.4.1 below. This specification uses its own requirements notation as described in Section 2.4.2 below.

In this specification, the term "data dictionary" refers to Annex L of [CPA] with the additions and modifications in Section 21 of this document.

2.4.1 Notation

In accordance with the EMV specification (e.g. [EMV 3], Section 5, Annexes A and B), the following notation is used for data description in this specification:

- An item of information is called a **data element**. A data element is the smallest piece of information that may be identified by a name, a description of logical content, a format, and a coding.
- A **data object** consists of a tag, a length, and a value (TLV). The value field of a data object may consist of either a single data element or one or more data objects. When a data object encapsulates a single data element, it is called a **primitive data object**. When a data object encapsulates one or more data objects, it is called a **constructed data object**. The value field of a constructed data object is called a **template**.

The names of templates and data elements defined in the data dictionary and used in this specification are written in italics to distinguish them from the text, e.g.

Application Control

In addition to or as replacement of those described in Section 4.2 of [CPA], the notational conventions described below are used in this specification.

'Name of Sub-Element' in *Data Object Name*	Reference to a sub-element of a data object defined in the data dictionary, e.g. 'Include Based on Transaction CVM' in *Counter x Control* = Include if Transaction CVM is No CVM
A <> B	Value of A is different from the value of B.
A <= B	Value of A is less than or equal to the value of B.
A >= B	Value of A is greater than or equal to the value of B.
A XOR B	The bit-wise exclusive-OR of the data blocks A and B. If one data block is shorter than the other then it is first padded to the left with sufficient binary zeros to make it the same length as the other.
[x:y]	Range of bytes of the referenced data element. For example, *Application Control*[1:3] represents bytes 1, 2, and 3 of the *Application Control*
[bx:y]	Range of bits of the referenced data element. For example, *Counter 1*[b4:1] represents bits 4, 3, 2, and 1 of *Counter 1*

2.4.2 Requirement Notation

The CPACE application shall comply with the requirements specified in this document that are labelled **Req C.x**.

Requirements are identified and numbered in bold. Heading and description of a requirement are marked by a frame:

Req C.x	**Requirement heading**
Requirement description	

3 General Requirements

3.1 Introduction

An instance of the CPACE application may co-exist with other instances of the CPACE application or with other applications on the same CPACE card. PSE and PPSE are examples of such other co-resident applications (see Section 3.4).

In addition, a CPACE application may be accessed on the contact or contactless interface and, since this specification requires that it is possible to assign several AIDs to a CPACE application (see Req C.2), several AIDs may be used to select a CPACE application, including consecutive selections with the "select next" option.

This specification assumes that the CPACE card is the central coordinator of interfaces and applications. In this role, the CPACE card:

- Handles the interfaces on which the card is accessed,
- Handles and dispatches the commands received over the respective interface.

In particular, in order to dispatch the SELECT command correctly, the CPACE card has to keep an inventory of the AIDs which are selectable with the SELECT command and of the applications these AIDs are assigned to.

Several requirements described in this section refer to the CPACE card in this central role.

3.2 Card Blocked

The following requirement is moved here from Section 7.3.2 of [CPA].

Req C.1	**Card blocked**
If the CPACE card is blocked, the card will discontinue processing the SELECT command and respond with SW1 SW2 = '6A81' (Function not supported).	

3.3 Handling of AIDs and SELECT Command

Req C.2	**Support of several AIDs**
Issuers shall have the option to have several instances of the CPACE application on the CPACE card (if allowed by the memory available on the card) and to assign up to 32 AIDs to each of these instances of the CPACE application. All AIDs assigned to an instance of the CPACE application shall be selectable with the SELECT command using the full or partial name.	

Note:

One of the AIDs assigned to a CPACE application is considered as the basic AID, which is used to personalise the application using CPS. The issuer shall have the option to personalise up to 31 additional AIDs for a CPACE application.

Req C.3	**Handling of selection with full or partial name**

The CPACE card shall keep an inventory of the AIDs of all its applications which are selectable with the SELECT command and of the application each AID is assigned to.

In particular, if several AIDs are assigned to a CPACE application, all these AIDs shall be kept in the CPACE card's inventory as assigned to the CPACE application.

If the CPACE card receives a SELECT command, the CPACE card shall compare the file name in the data field of the SELECT command to the AIDs in its inventory of AIDs. If the file name matches (the first bytes of) an AID, the AID is eligible for selection.

It may occur, that several AIDs in the inventory of the CPACE card are eligible for selection. Therefore, the CPACE card shall be able to decide, which of potentially several AIDs, that are eligible for selection, is to be selected for a SELECT command with the "select first or only" option. In addition, the CPACE card shall be able to handle the sequence in which several AIDs, that are eligible for selection, are to be selected for successively received SELECT commands with the same file name and "select next" option.

If the CPACE card decides that an AID assigned to a CPACE application is to be selected, the CPACE card shall forward the SELECT command to the CPACE application. In addition to forwarding the SELECT command containing the file name in its data field, the CPACE card shall provide information to the CPACE application of the AID to be selected. According to the rules stated above, the AID to be selected is an AID assigned to the CPACE application which begins with, but may be longer than the file name in the data field of the SELECT command.

Depending on the card platform, if the CPACE card receives a SELECT command containing a file name which does not match (the first bytes of) any of the AIDs in the CPACE card's inventory, the CPACE card may either reject the SELECT command or forward the SELECT command to the currently selected application.

If the CPACE card decides to forward such a SELECT command to a (currently selected) CPACE application, the CPACE card shall provide information to the CPACE application that the file name in the data field of the SELECT command does not match (the first bytes of) any of the AIDs assigned to the CPACE application.

3.4 Support of PPSE and PSE

Req C.4	**Support of PPSE**
The CPACE card shall support the PPSE, as specified in [EMV B].	

Req C.5	**Support of PSE**
The CPACE card shall support the PSE as specified in [EMV 1].	

Note:

It should be possible to adapt the PPSE and the PSE on dual interface cards in order to take into account that applications have been blocked.

In addition, it should be possible to adapt the PPSE on dual interface cards in order to take into account that contactless access to applications has been deactivated.

Preferably, applications should be removed from/added to the PPSE and the PSE internally when applications are blocked/unblocked and applications should be removed from/added to from the PPSE when contactless access to the applications is deactivated/activated.

It is left to the implementer if and how to realise such mechanisms.

3.5 Handling of Interfaces

Req C.6	**No concurrent access on both interfaces**
The CPACE card shall prevent concurrent access to any application, in particular to any CPACE application, using a different interface than the currently active interface.	

Note:

This specification assumes that Req C.6 is met by the CPACE card and that the CPACE application does not receive a command on the contact interface while it is currently selected on the contactless interface and vice versa.

Req C.7	**Identification of the interface in use**
The CPACE application shall be able to distinguish which interface, contactless or contact, is currently used.	

Note:

According to this specification, the interface in use is identified during SELECT command processing (see Section 6.3.4).

3.5.1 Activation and Deactivation of Contactless Access to the CPACE Application

According to this specification, mechanisms are required which allow activation and deactivation of contactless access to the CPACE application on dual interface cards.

Note:

For dual interface cards, if the Activation/Deactivation of Contactless Access to Dual Interface Cards implementer-option is supported, activation and deactivation of contactless access to the CPACE card shall be possible (see Section 3.5.2). This has effect on all applications supported by the card, while the mechanisms described in this section apply to a single CPACE application.

Req C.8	**Contactless access to application activated/deactivated set by issuer**
The CPACE application shall support a mechanism that allows the issuer to specify if contactless access to the CPACE application is activated or deactivated. If the Contactless Control - Application implementer-option is supported, then 'State of contactless access to the application' in *Contactless Control - Application* shall be used to specify if contactless access to the CPACE application is activated or deactivated. If, by means of this mechanism, contactless access to the CPACE application is deactivated, then selection and initiation of the CPACE application on the contactless interface shall be denied according to Req C.33 and Req C.43.	

Note:

Normally, the CPACE application transitions to the state **SELECTED** from a state where it is not currently selected upon successful processing of the SELECT command.

Therefore, denying selection of the CPACE application if contactless access to the CPACE application or, if the Activation/Deactivation of Contactless Access to Dual Interface Cards implementer-option is supported, to the CPACE card is deactivated, prevents the CPACE application from transitioning to the state SELECTED if it is not currently selected. According to its state machine (see Section 5.2), the CPACE application can only be used to perform a transaction if it is able to transition to the state SELECTED. Therefore, if contactless access to the CPACE application or to the CPACE card is deactivated denying selection of the CPACE application is sufficient to prevent

transaction processing on the contactless interface provided the CPACE application is in a state where it is not currently selected.

But, according to the definition of its state machine (see Section 6.2.2 of [CPA]), the CPACE application also transitions to or remains in the state **SELECTED** if either of the following is true:

- If an error occurs in command processing for GENERATE AC or GET PROCESSING OPTIONS, in a state in which the command is allowed, the application shall transition to the **SELECTED** state
- For an error in processing any other command which is allowed in the **SELECTED** state, the CPACE application shall remain in the **SELECTED** state.

In particular, if the CPACE application is already selected on the contactless interface, denying selection of the CPACE application if contactless access to the CPACE application or to the CPACE card is deactivated does not prevent transaction processing on the contactless interface for the CPACE application.

Therefore, it is also required according to this specification, that if contactless access to the CPACE application or to the CPACE card is deactivated, the GET PROCESSING OPTIONS command shall be rejected if processed in the state **SELECTED** on the contactless interface.

Req C.9	**Activation of contactless access to application by issuer**
The CPACE application shall support a mechanism (issuer activation of contactless access) that allows the issuer to perform a script command or to use a CSU mechanism with the second GENERATE AC command to activate contactless access to the CPACE application. Issuer activation of contactless access to the CPACE application shall disable the mechanism for unsecured (re-)deactivation of contactless access to the application described in Req C.12. If the Contactless Control - Application implementer-option is supported, then the CPACE application shall support the CSU mechanism according to Req C.107 and Req C.110 and the ACTIVATE CL script command according to the command specification in Section 14.6 in order to implement compliance with this requirement.	

Req C.10	**Deactivation of contactless access to application by issuer**
The CPACE application shall support a mechanism (issuer deactivation of contactless access) that allows the issuer to perform a script command on the contact or contactless interface or to use a CSU mechanism with the second GENERATE AC command on the contact or contactless interface to deactivate contactless access to the CPACE application. Issuer deactivation of contactless access to the CPACE application shall disable any mechanism for implicit activation of contactless access to the application described in Req C.11. If the Contactless Control - Application implementer-option is supported, the CPACE application shall support the CSU mechanism according to Req C.107 and Req C.111 and the DEACTIVATE CL script command according to the command specification in Section 14.7 in order to implement compliance with this requirement.	

Note:

- If issuer deactivation of contactless access to the CPACE application is performed on the contactless interface, subsequent SELECT commands and subsequent GET PROCESSING OPTIONS commands performed for the application shall be denied according to Req C.33 and Req C.43. But other commands may still be processed on the contactless interface as long as the current CPACE application remains selected on the contactless interface, provided the respective command is permitted according to the state machine of the CPACE application.
- If the Contactless Control - Application implementer-option is supported, activation and deactivation of contactless access to the CPACE application may also be done by updating *Contactless Control - Application* with a PUT DATA command (see Section 14.4).
- If the Contactless Control - Application implementer-option is supported and if contactless access to the CPACE application is activated according to 'State of contactless access to the application' in *Contactless Control - Application*, then contactless access to the CPACE application can be deactivated on the contactless interface using the second GENERATE AC command or the DEACTIVATE CL script command. Afterwards, (additional) script commands or, if contactless access is deactivated with the DEACTIVATE CL command, the second GENERATE AC command can still be processed on the contactless interface.
- If the Contactless Control - Application implementer-option is supported and if contactless access to the CPACE application is deactivated according to 'State of contactless access to the application' in *Contactless Control - Application*, then successful processing of the second GENERATE AC command and of the ACTIVATE CL script command is normally only possible on the contact interface. But the second GENERATE AC command and the ACTIVATE CL script command can be processed successfully on the contactless interface, if contactless access to the application has been deactivated during the same transaction with the DEACTIVATE CL script command or with the second GENERATE AC command.

The issuer shall have the option to deactivate contactless access to the CPACE application during card delivery and to specify that contactless access to the CPACE application is activated under a certain condition when a contact transaction is performed.

Req C.11	**Activation of contactless access to application with (first) contact transaction**
The CPACE application shall support a mechanism (implicit activation of contactless access) that activates contactless access to the CPACE application when a transaction for the CPACE application on the contact interface is performed. The CPACE application shall support a mechanism which allows the issuer to specify if implicit activation of contactless access to the CPACE application is enabled or disabled. If the Contactless Control - Application implementer-option is supported, 'Activation of contactless access to the application with SELECT of the application on the contact interface' in *Contactless Control - Application* shall be used to specify if implicit activation of contactless access to the CPACE application is enabled or disabled. If implicit activation of contactless access to the CPACE application is enabled, contactless access to the CPACE application shall be activated as described in Req C.39. If the Contactless Control - Application implementer-option is supported, the CPACE application shall support additional mechanisms for implicit activation of contactless access to the CPACE application as described in Req C.75 and Req C.106.	

For testing purposes during card personalisation, after performing tests on the contact or contactless interface, a mechanism is needed to put the CPACE application (back) to the state where contactless access is deactivated. This mechanism must not require issuer interaction. The issuer shall have the option to enable or disable this mechanism.

Req C.12	**Deactivation of contactless access to application after testing**

The CPACE application shall support a mechanism (unsecured (re-)deactivation of contactless access) that (re-)deactivates contactless access to the CPACE application without issuer interaction.

In addition, if the mechanism for unsecured (re-)deactivation of contactless access to the CPACE application is performed on the contactless interface, subsequent commands on the contactless interface shall be denied by the CPACE application.

It shall be possible to disable the mechanism for unsecured (re-)deactivation of contactless access to the CPACE application without issuer interaction on the contact interface or on the contactless interface.

The CPACE application shall support a mechanism which allows the issuer to specify if the mechanism for unsecured (re-)deactivation of contactless access to the application is enabled or disabled.

If the Contactless Control - Application implementer-option is supported, the CPACE application shall support the unsecured DEACTIVATE CL command according to the command specification in Section 14.7 to implement compliance with this requirement. In particular,

3.5.2 Activation and Deactivation of the Contactless Access to Dual Interface Cards

For dual interface cards, if the Activation/Deactivation of Contactless Access to Dual Interface Cards implementer-option is supported, the mechanisms described in this section are required which allow activation and deactivation of contactless access to the CPACE card.

Req C.13	**Contactless access to card activated/deactivated set by issuer**

The CPACE card shall support a mechanism that allows the issuer to specify if contactless access to the CPACE card is activated or deactivated.

If the Contactless Control - Card implementer-option is supported, 'State of contactless access to the card' in *Contactless Control - Card* shall be used to specify if contactless access to the CPACE card is activated or deactivated.

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.

Req C.14	**Right to activate/deactivate contactless access to card assigned to application by issuer**

The CPACE card and the CPACE application shall support a mechanism that allows the issuer to specify individually for each CPACE application if it has the right to activate/deactivate contactless access to the card.

If the Contactless Control - Application implementer-option is supported 'Right of application to activate/deactivate contactless access to the card' in *Contactless Control - Application* shall be used to specify if the application has the right to activate/deactivate contactless access to the card.

If, by means of this mechanism, a CPACE application has the right to activate/deactivate contactless access to the card, then the respective application shall have the right to activate and to deactivate contactless access to the card as described in Req C.15, Req C.16, Req C.17 and Req C.18.

Note:

- The Contactless Control - Application implementer-option must be supported when the Contactless Control - Card implementer-option is supported (see Section 4.2.2). Therefore, if the Contactless Control - Card implementer-option is supported 'Right of application to activate/deactivate contactless access to the card' in *Contactless Control - Application* shall be used to specify if the application has the right to activate/deactivate contactless access to the card.
- The right to activate/deactivate contactless access to the card implies control of contactless access by individual applications for all other applications on the CPACE card.

Req C.15	**Activation of contactless access to card by issuer**

The CPACE card and the CPACE application shall support a mechanism (issuer activation of contactless access) that allows the issuer to perform a script command on the contact interface or to use a CSU mechanism with the second GENERATE AC command on the contact interface to activate contactless access to the CPACE card, provided the currently selected CPACE application has the right to activate/deactivate contactless access to the card.

Issuer activation of contactless access to the CPACE card shall disable the mechanism for unsecured (re-)deactivation of contactless access to the card described in Req C.18.

If the Contactless Control - Card implementer-option is supported, the CPACE card and the CPACE application shall support the CSU mechanism according to Req C.107 and Req C.108 and the ACTIVATE CL script command according to the command specification in Section 14.6 in order to implement compliance with this requirement.

Req C.16	**Deactivation of contactless access to card by issuer**

The CPACE card and the CPACE application shall support a mechanism (issuer deactivation of contactless access) that allows the issuer to perform a script command on the contact or contactless interface or to use a CSU mechanism with the second GENERATE AC command on the contact or contactless interface to deactivate contactless access to the CPACE card, provided the currently selected CPACE application has the right to activate/deactivate contactless access to the card.

Issuer deactivation of contactless access to the CPACE card shall take effect on the next card session, i.e. the contactless interface of the CPACE card shall be mute on the attempt to start the next card session. In addition, if issuer deactivation of contactless access to the CPACE card is performed on the contactless interface, subsequent selection and initiation of any CPACE application on the contactless interface shall be denied according to Req C.33 and Req C.43.

Issuer deactivation of contactless access to the CPACE card shall disable any mechanism for implicit activation of contactless access to the card described in Req C.17.

If the Contactless Control - Card implementer-option is supported, the CPACE application shall support the CSU mechanism according to Req C.107 and Req C.109 and the DEACTIVATE CL script command according to the command specification in Section 14.7 in order to implement compliance with this requirement.

Note:

- If issuer deactivation of contactless access to the CPACE card is performed on the contactless interface, subsequent SELECT commands and subsequent GET PROCESSING OPTIONS commands performed for any CPACE application shall be denied according to Req C.33 and Req C.43. But other commands may still be processed on the contactless interface as long as the current CPACE application remains selected on the contactless interface, provided the respective command is permitted according to the state machine of the CPACE application.
- If the Contactless Control - Card implementer-option is supported, activation and deactivation of contactless access to the CPACE application may also be done by updating *Contactless Control - Card* with a PUT DATA command (see Section 14.4).

The issuer shall have the option to deactivate contactless access to the CPACE card during card delivery and to specify that contactless access to the CPACE card is activated under a certain condition when a contact transaction is performed, provided the currently selected CPACE application that has the right to activate/deactivate contactless access to the card.

Req C.17	**Activation of contactless access to card with (first) contact transaction**

The CPACE card and the CPACE application shall support a mechanism (implicit activation of contactless access) that activates contactless access to the CPACE card when a transaction on the contact interface is performed, provided the currently selected CPACE

application has the right to activate/deactivate contactless access to the card.

The CPACE card shall support a mechanism which allows the issuer to specify if implicit activation of contactless access to the CPACE card is enabled or disabled.

If the Contactless Control - Card implementer-option is supported, 'Activation of contactless access to the application with SELECT of an application on the contact interface' in *Contactless Control - Card* shall be used to specify if implicit activation of contactless access to the CPACE card is enabled or disabled.

If implicit activation of contactless access to the CPACE card is enabled, contactless access to the CPACE application shall be activated as described in Req C.38.

If the Contactless Control - Card implementer-option is supported, the CPACE card and the CPACE application shall support additional mechanisms for implicit activation of contactless access to the CPACE card as described in Req C.74 and Req C.105.

For testing purposes during card personalisation, after performing tests on the contact or contactless interface, a mechanism is needed to put the CPACE card (back) to the state where contactless access is deactivated. This mechanism must not require issuer interaction. The issuer shall have the option to enable or disable this mechanism.

Req C.18 Deactivation of contactless access to card after testing

The CPACE card and the CPACE application shall support a mechanism (unsecured (re-)deactivation of contactless access) that (re-)deactivates contactless access to the CPACE card without issuer interaction, provided the currently selected CPACE application has the right to activate/deactivate contactless access to the card.

In addition, if the mechanism for unsecured (re-)deactivation of contactless access to the CPACE card is performed on the contactless interface, subsequent commands on the contactless interface shall be denied by any CPACE application.

It shall be possible to disable the mechanism for unsecured (re-)deactivation of contactless access to the CPACE card without issuer interaction on the contact interface or on the contactless interface.

The CPACE card shall support a mechanism which allows the issuer to specify if the mechanism for unsecured (re-)deactivation of contactless access to the card is enabled or disabled.

If the Contactless Control - Card implementer-option is supported, the CPACE card and the CPACE application shall support the unsecured DEACTIVATE CL command according to the command specification in Section 14.7 to implement compliance with this requirement.

3.6 Logical Channels

Req C.19	Logical channels
Like [CPA], this specification describes only logical channel 0 for command APDUs. This implies that the CPACE application shall reject any command sent on a logical channel different from 0 according to Req 6.3 in [CPA], and therefore concurrent access to a CPACE application on several logical channels is not allowed.	

Note:

Req C.19 refers to the CPACE application, not to the CPACE card. It is still allowed that the CPACE card supports multiple logical channels.

3.7 Data Sharing

Req C.20	Data sharing
It shall be possible to share Reference PIN, PIN Try Limit and PIN Try Counter between CPACE applications and non-CPACE applications on the same card.	

Note:

Since the CPACE application supports a powerful Profile Selection mechanism based on AID and interface in use, data can be shared by assigning several AIDs to the same CPACE application, sharing data by assigning them to several of the profiles used for the different AIDs and keeping data separate by assigning them only to one of the profiles used for the different AIDs.

3.8 Performance Requirements

Req C.21	Performance requirements
CPACE implementations shall meet the performance requirements for cards according to Section 10 of [EMV A]. Currently this implies a card tariff of 400ms for the card processing of a payment.	

Note:

Adherence to Req C.21 will be tested with CPACE application profiles defined according to the implementation requirements of CPACE card issuers.

4 Overview and Additional Functionality

4.1 Introduction

This section refers to Section 5 and 19 of [CPA]:

- Additional requirements and modifications regarding Section 5.1 of [CPA] (Implementer-Options) are described in Section 4.2.
- Additional requirements regarding Section 5.4.2 of [CPA] (Command Support Requirements) are described in Section 4.3.
- Additional Functionality, as defined in Section 19 of [CPA], supported by the CPACE application is listed in Section 4.4.
- Section 4.5 refers to an extension (Relay Resistance Protocol) of [CPA] which is still to be fully integrated in this specification.

4.2 Implementer-Options

4.2.1 CPA Implementer-Options

The implementer-options

- Dynamic-RSA,
- Profile Selection Using Card Data,
- Application Security Counters,
- Cryptogram Version '5'-only,
- Cryptogram Version '6'-only,
- Cryptogram Version '5' and '6'

defined in Section 5.1 of [CPA] (including the extensions according to Specification Bulletin 165) shall be supported for the CPACE application according to the following requirements.

Req C.22	**Support of Dynamic-RSA**
The CPACE application shall support the Dynamic-RSA implementer-option defined in [CPA].	

Req C.23	**Support of Profile Selection Using Card Data**
The CPACE application shall support the Profile Selection Using Card Data implementer-option defined in [CPA] as described in Section 6.2.	

Req C.24	**Support of Application Security Counters**
If the CPACE application supports the Application Security Counters implementer-option, then security counters shall be implemented within the application as described in Section 18 of this specification.	

Req C.25	**Support of Cryptogram Versions '5' and/or '6'**
The CPACE application shall support either the Cryptogram Version '5'-only implementer-option or the Cryptogram Version '6'-only implementer-option or the Cryptogram Version '5' and '6' implementer-option as described in Specification Bulletin 165. If the Cryptogram Version '5' and '6' implementer-option is supported, according to Specification Bulletin 165, an instance of the CPACE application is only expected to use one of the cryptographic algorithms at a time, either Triple DES or AES. It is the issuer's decision, which cryptographic algorithm is used for an instance of the CPACE application, by personalising either Triple DES or AES versions of the master keys for the instance of the CPACE application.	

4.2.2 CPACE Implementer-Options

For the CPACE application, additional implementer-options are defined by this specification and functionality defined as mandatory in [CPA] is defined as an implementer-option by this specification. These additional implementer-options are numbered **IOn** and listed in Table 2.

Implementer-Option		**Description**
IO1	**Activation/Deactivation of Contactless Access to Dual Interface Cards**	A CPACE implementation on a dual interface card that supports this implementer-option shall support a mechanism that allows the issuer to specify if access to the dual interface card on the contactless interface is activated or deactivated.

Implementer-Option	Description
IO2: Contactless Control - Application	A CPACE implementation on a dual interface card that supports this implementer-option shall use the *Contactless Control - Application* data element to: • Control activation and deactivation of contactless access to the application, • Indicate, whether the application has the right to activate/deactivate contactless access to the card. It is mandatory to support the Contactless Control - Application implementer-option if the Contactless Control - Card implementer-option is supported. But the Contactless Control - Application implementer-option may be supported without supporting the Contactless Control - Card implementer-option, even if the Activation/Deactivation of Contactless Access to Dual Interface Cards implementer-option is supported.
IO3: Contactless Control - Card	A CPACE implementation on a dual interface card supporting the Activation/Deactivation of Contactless Access to Dual Interface Cards implementer-option that supports this implementer-option shall use the *Contactless Control - Card* data element to control activation and deactivation of contactless access to the card. Support of the Contactless Control - Card implementer-option implies support of the Contactless Control - Application implementer-option.
IO4: Contactless Command Access Controls	A CPACE implementation that supports this implementer-option shall use the *Contactless Command Access*, the *Contactless READ RECORD Access* and the *Contactless GET DATA Access* in the *Contactless Command Access Controls* template to control access of commands to the CPACE application on the contactless interface.

Implementer-Option	Description
IO5 Internal Data Logging	A CPACE implementation that supports this implementer-option shall use • The Environment in Use data element to store the interface in use and • The *Internal Log Data Object List (ILDOL)* in the *Log Data Tables* template to log additional transaction data internal to the CPACE application.
IO6: Other MAC Lengths	A CPACE implementation that supports this implementer-option shall support 4-byte to 8-byte MACs according to Section 19.3.7 of [CPA]
IO7: Additional Master Keys	A CPACE implementation that supports this implementer-option shall support personalisation and usage of 15 additional sets of Triple DES master keys, each consisting of *Additional Master Key for AC x*, *Additional Master Key for SMI x*, *Additional Master Key for SMC x*. If the Cryptogram Version '5' and '6' or Cryptogram Version '6'-only implementer-option is supported, a CPACE implementation that supports this implementer-option shall also support personalisation and usage of 15 additional sets of AES master keys, each consisting of *Additional Master Key for AC x*, *Additional Master Key for SMI x*, *Additional Master Key for SMC x*. The set of master keys to be used during a transaction shall be identified by the *Profile Control x* selected during Profile Selection.
IO8: Relay Resistance Protocol	A CPACE implementation that supports this implementer option shall support a Relay Resistance Protocol according to Req C.27.

Table 2: Additional Implementer-Options for CPACE Implementations

4.3 Command Support Requirements

Req C.26	**Additional supported commands**

In addition to the commands listed in Table 5-3 of [CPA], the CPACE application

- Shall support the mandatory commands listed in Table 3,
- Shall support the conditional commands listed in Table 3 if the associated condition is true.

Command	CLA	INS	CPACE Support
ACTIVATE CL	'EC'	'44'	Conditional - If Contactless Control - Card and/or Contactless Control - Application implementer-option is supported
DEACTIVATE CL (unsecured)	'E0'	'04'	Conditional - If Contactless Control - Card and/or Contactless Control - Application implementer-option is supported
DEACTIVATE CL (script)	'EC'	'04'	Conditional - If Contactless Control - Card and/or Contactless Control - Application implementer-option is supported
EXCHANGE RELAY RESISTANCE DATA (ERRD)	'80'	'EA'	Conditional - If Relay Resistance Protocol implementer-option is supported

Table 3: Additional Command Support Requirements

4.4 Additional Functionality

According to this specification, the CPACE application shall support additional functionality either unconditionally or as implementer-option. It is an issuer option to use the additional functionality. With the exception of Other MAC Lengths, the additional functions are controlled by parameters of the CPACE application. In particular, additional functions are switched on or off by the appropriate setting of these parameters. If all parameters are set as described in [CPA], the additional functions except Other MAC Lengths are switched off.

The additional functions supported by the CPACE application are listed in Table 4 together with the parameters that control the respective function.

Additional Function	**Control Parameters**
Use additional accumulator and/or counter	*Application Control*, *Profile Control*
Issuer Discretionary Data in the Issuer Application Data: • Additional *Accumulator, Counter,* • Offline Transactions End Date, • *Static Issuer Data*, • *Dynamic Issuer Data*	*Application Control*, *Profile Control*, *Issuer Options Profile Control*
Proprietary Authentication Data in *IATD* and individual update of accumulators and counters	*Issuer Options Profile Control*
Cashback Check to force cashback transactions online (usage of an issuer discretionary bit in *ADR* and CIACs)	*Issuer Options Profile Control*
Usage of an issuer discretionary bit for Terminal Erroneously considers Offline PIN OK in the *CVR*	*Issuer Options Profile Control*
Profile Selection Based on the Status of Accumulators and Counters using Extended Check Types	*Application Control*, Bit b8 of Check Type in Profile Selection Entries
Accumulation and Counting Based on *Transaction CVM*	*Application Control*, Extended *Accumulators Controls*, Extended *Counters Controls*
Accumulation, Counting and Logging of Online Requests	*Application Control*, Extended *Accumulators Controls,* Extended *Counters Controls*
Reset of Accumulators and Counters on Offline PIN Verification	*Application Control*, Extended *Accumulators Profile Controls,* Extended *Counters Profile Controls*
Activation and Deactivation of Contactless Access to Dual Interface Cards, if the Activation/Deactivation of Contactless Access to Dual Interface Cards implementer-option is supported	*Contactless Control - Card*, if the Contactless Control - Card implementer-option is supported, implementation specific control, if the Contactless Control - Card implementer-option is not supported
Activation and Deactivation of Contactless Access to the CPACE Application	*Contactless Control - Application*, if the Contactless Control - Application implementer-option is supported, implementation specific control, if the Contactless Control - Application implementer-option is not supported

Additional Function	Control Parameters
Contactless command access control	*Contactless Command Access Controls* template, containing *Contactless Command Access*, *Contactless READ RECORD Access* and *Contactless GET DATA Access*, if the Contactless Command Access Controls implementer-option is supported, implementation specific control, if the Contactless Command Access Controls implementer-option is not supported
Internal Data Logging and *Environment in Use* data element, if implementer-option Internal Data Logging is supported	*Internal Log Data Object List (ILDOL)* in the *Log Data Tables* template
AES, if implementer-option Cryptogram Version '5' and '6' or Cryptogram Version '6'-only is supported	Personalisation of either the Triple DES version or the AES version of the master keys, CCI in the *Issuer Options Profile Control*
Other MAC Lengths, if implementer-option Other MAC Lengths is supported	Issuer choice to use 4-byte to 8-byte MACs
First GENERATE AC response with CDA on AAC if requested on the contactless interface	Required (see Req C.98)
Additional *GPO Parameters x*	Personalisation of additional *GPO Parameters x*, identified by the tags 'DF10' to 'DF7E'
Additional sets of master keys, if implementer-option Additional Master Keys is supported	Personalisation of additional set(s) of master keys
Relay Resistance Protocol, if implementer-option Relay Resistance Protocol is supported	*Issuer Options Profile Control*

Table 4: Additional Functionality of a CPACE Application

4.5 Relay Resistance Protocol

If the Relay Resistance Protocol implementer-option is supported, the CPACE application shall support a Relay Resistance Protocol based on the evaluation of the time it takes for the CPACE application to process the EXCHANGE RELAY RESISTANCE DATA (ERRD) command. The time measurement is made by the terminal and it is compared to the timing limits provided to the terminal in the response data field of the ERRD command.

Req C.27	**Relay Resistance Protocol**

If the Relay Resistance Protocol implementer-option is supported, the CPACE application shall support:

- The ERRD command (see Req C.26, Section 5.2 and Section 8),
- Additional steps in GET PROCESSING OPTIONS command processing necessary to prepare ERRD command processing (see Section 7.2.5),
- An additional check and a modification of dynamic signature generation in first GENERATE AC command processing necessary to protect the results of ERRD command processing from unauthorised changes (see Sections 12.2.3.4 and 12.2.7.4),
- Additional and modified data necessary to personalise and perform Relay Resistance Protocol processing (see Sections 21.19, 21.21, 21.22, 21.33, 21.34, 21.38, 21.42, 21.47, 21.48, 21.53, 21.54, 21.55, 21.56, 21.57, 21.64).

Currently, the Relay Resistance Protocol is only supported for contactless transactions. In the future, the Relay Resistance Protocol may be extended to contact transaction processing. If the Relay Resistance Protocol implementer-option is supported, a bit in the Proprietary Issuer Options Profile Parameters part of the *Issuer Options Profile Control* indicates whether the Relay Resistance Protocol shall be performed for a transaction.

5 General Command Information

5.1 Introduction

This section refers to Section 6 of [CPA]:

- Modifications regarding Section 6.2 of [CPA] (State Machine) are described in Section 5.2.
- Additional requirements regarding Section 6.3 of [CPA] (Command Validation) are described in Section 5.3.

5.2 State Machine

The following Table 5, which is an extension of Table 6-2 in [CPA] including the commands that shall or may be supported by the CPACE application, shows the sequence of commands and transitions between the states of the CPACE application, after the application state was initialised to SELECTED either by a successfully executed SELECT command or after an error has occurred in command processing which causes a transition to SELECTED.

State ⇒ **Command ⇓**	**SELECTED**	**INITIATED**	**ONLINE**	**SCRIPT**
ACTIVATE CL	Not Allowed	Not Allowed	**ONLINE**	**SCRIPT**
APPLICATION UNBLOCK	Not Allowed	Not Allowed	**ONLINE**	**SCRIPT**
DEACTIVATE CL (script)	Not Allowed	Not Allowed	**ONLINE**	**SCRIPT**
DEACTIVATE CL (unsecured)[1)]	**SELECTED**	**SELECTED**	**SELECTED**	**SELECTED**
EXCHANGE RELAY RESISTANCE DATA	Not Allowed	**INITIATED**	Not Allowed	Not Allowed

[1)] The unsecured DEACTIVATE CL command should have been disabled before the CPACE card leaves the personalisation environment.

State ⇒ Command ⇓	SELECTED	INITIATED	ONLINE	SCRIPT
GENERATE AC	Not Allowed	**SCRIPT** (if response is TC or AAC and SW1 SW2 = '9000') **ONLINE** (if response is ARQC and SW1 SW2 = '9000') **SELECTED** (if SW1 SW2 <> '9000')	**SCRIPT** (if SW1 SW2 = '9000') **SELECTED** (if SW1 SW2 <> '9000')	Not Allowed
GET CHALLENGE	**SELECTED**	**INITIATED**	**ONLINE**	**SCRIPT**
GET DATA	**SELECTED**	**INITIATED**	**ONLINE**	**SCRIPT**
GET PROCESSING OPTIONS	**INITIATED** (if SW1 SW2 = '9000') **SELECTED** (if SW1 SW2 <> '9000')	Not Allowed	Not Allowed	Not Allowed
INTERNAL AUTHENTICATE	Not Supported	**INITIATED**	Not Supported	Not Supported
PIN CHANGE/ UNBLOCK	Not Allowed	Not Allowed	**ONLINE**	**SCRIPT**
PUT DATA	Not Allowed	Not Allowed	**ONLINE**	**SCRIPT**
READ RECORD	**SELECTED**	**INITIATED**	**ONLINE**	**SCRIPT**
SELECT	**SELECTED**	**SELECTED**	**SELECTED**	**SELECTED**
UPDATE RECORD	Not Allowed	Not Allowed	**ONLINE**	**SCRIPT**
VERIFY	Not Supported	**INITIATED**	Not Supported	Not Supported

Table 5: Sequence of Commands and State Transitions for Commands

5.3 Command Validation

The following requirement is added at the beginning of Section 6.3 of [CPA].

Req C.28	**Rejection of incorrect command APDUs**

If the CPACE application receives a command APDU which is not coded correctly according to Section 11.1.1 of [EMV 1], the CPACE application shall reject the command APDU, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6700' (Wrong Length). This includes rejection of command APDUs where the value of Lc is different from the actual length of data.

In addition, command APDUs with a length of less than 4 bytes received by the CPACE application shall not invalidate a challenge which has been generated for the CPACE application with a GET CHALLENGE command.

Note:

According to this specification, it is allowed that the CPACE card rejects command APDUs which are not coded correctly according to Section 11.1.1 of [EMV 1].

In this case, the CPACE application will receive only correctly coded command APDUs and incorrectly coded command APDUs will not invalidate a challenge which has been generated for the CPACE application with a GET CHALLENGE command.

The following requirement is added at the end of Section 6.3 of [CPA].

Req C.29	**Validation of command case and Le**

If the CPACE application receives a known command, i.e. command validation according to Req 6.3 in Section 6.3 of [CPA] has been passed successfully, and **any** of the following is true:

- the command message contains a command data field, but the command does not expect command data,
- **or** Le is present in the command message, but the command does not return data in its response according to its definition in [CPA] or in the specification,
- **or** Le is present in the command message but has another value than '00',

then the CPACE application shall discontinue processing the command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6700' (Wrong Length).

If Le <> '00' is detected in command processing for GENERATE AC or GET PROCESSING OPTIONS, in a state in which the command is allowed, the CPACE application shall transition to the SELECTED state.

If a wrong command case or Le <> '00' is detected in processing any other command, the application shall remain in the current state.

6 Application Selection

6.1 Introduction

This section refers to Section 7 of [CPA]:

- Additional requirements and modifications regarding Section 7.3.2 of [CPA] (Identifying and Selecting the Application) are described in Section 6.2.
- Requirements previously contained in Section 7.3.2 of [CPA] and additional requirements are described in the new Section 6.3 (SELECT Command).

6.2 Identifying and Selecting the Application

Paragraphs 4 and 5 are moved from Section 7.3.2 of [CPA] to Req C.40 and Req C.36 in Section 6.3.4.

Paragraph 6 is moved from Section 7.3.2 of [CPA] to Req C.1 in Section 3.2.

Req 7.2 and the paragraph preceding it in Section 7.3.2 of [CPA] are replaced with the following Req C.30.

Req C.30	**Support of AID-Interface Table**
The CPACE application shall support the AID-Interface Table as defined in Sections 9.3.3.2 and 21.17 so that issuers have the option to associate each AID (*DF Name*) assigned to the CPACE applications with different FCI per interface and with a different entry in the *GPO Parameters* template per interface.	

6.3 SELECT Command

6.3.1 Introduction

According to this specification, the SELECT command shall provide additional functionality to handle:

- The different interfaces on which the CPACE application may be accessed and
- The different AIDs which may be assigned to the CPACE application.

6.3.2 Command Coding

According to Section 11.3.2 of [EMV 1], the SELECT command message is coded as follows:

Code	Value
CLA	'00'
INS	'A4'
P1	'04': Select by name
P2	'00': First or only occurrence '02' Next occurrence
Lc	'05' - '10'
Data	File name
Le	'00'

Table 6: SELECT Command Message

Note:

- If the CPACE application is to be selected with the SELECT command, according to Req C.3, in addition to the SELECT command message, the CPACE application receives the information which of its AIDs is to be selected. In this case, the file name received in the data field of the SELECT command matches the (first bytes of) the AID to be selected.
- Depending on the card platform, when the CPACE application is already selected, it may occur that the CPACE application receives a SELECT command with a file name in its data field that does not match any of the AIDs assigned to the CPACE application.

6.3.3 Command Format Validation

Req C.31	**Check P1 and P2 for SELECT command**
If P1-P2 have none of the values specified for the SELECT command, then the application shall discontinue processing the command, shall respond with an SW1 SW2 indicating an error, and should respond with SW1 SW2 = '6A86' (Incorrect Parameters, P1-P2).	

Req C.32	**Check AID**

If the CPACE application receives a SELECT command, according to Req C.3, either of the following is true:

- The CPACE card provides information to the CPACE application that an AID assigned to the CPACE application is to be selected and which of the AIDs assigned to the CPACE application is the AID to be selected.

  In this case, the AID to be selected shall be stored in *AID*.

  Note:

  According to Req C.3, the AID to be selected, i.e. *AID*, begins with, but may be longer than the file name received in the SELECT command data field.

- The CPACE card provides information to the CPACE application that the file name received in the SELECT command data field does not match (the first bytes of) any of the AIDs assigned to the CPACE application.

  In this case, the CPACE application shall discontinue processing the command, shall respond with an SW1 SW2 indicating an error, and should respond with SW1 SW2 = '6A82' (File Not Found).

6.3.4 Processing

When the CPACE application receives a SELECT command with a file name in its data field which matches (the first bytes of) one of the AIDs assigned to the CPACE application, the command is processed as follows.

Req C.33	**Check contactless access activated/deactivated - SELECT**

If the interface currently used is contactless (see Req C.7), then the CPACE application shall check, whether contactless access to the CPACE application is deactivated (see Req C.8).

If the Contactless Control - Application implementer-option is supported, then 'State of contactless access to the application' in *Contactless Control - Application* shall be evaluated to check whether contactless access to the CPACE application is deactivated, i.e. 'State of contactless access to the application' in *Contactless Control - Application* = DEACTIVATED.

If the Activation/Deactivation of Contactless Access to Dual Interface Cards implementer-option is supported and if the interface currently used is contactless (see Req C.7), then the CPACE application shall check, whether contactless access to the CPACE card is deactivated (see Req C.13).

If the Contactless Control - Card implementer-option is supported, then 'State of contactless access to the card' in *Contactless Control - Card* shall be evaluated to check whether contactless access to the CPACE card is deactivated, i.e. 'State of contactless access to the Card' in *Contactless Control - Card* = DEACTIVATED.

If the interface currently used is contactless but contactless access to the CPACE application or to the CPACE card is deactivated, then, irrespective of which of the AIDs assigned to the CPACE application is used with the SELECT command, the CPACE application shall discontinue processing the SELECT command, shall respond with an SW1 SW2 that indicates an error (no FCI returned), and should respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

Req C.34 Retrieve *FCI Proprietary Template* and *GPO Parameters Reference*

The AID-Interface File shall be evaluated

- to retrieve the *FCI Proprietary Template* to be returned in the response to the SELECT command and
- to determine the *GPO Parameters Reference* to be used for GET PROCESSING OPTIONS command processing.

If any of the following errors is detected when the AID-Interface File is to be evaluated:

- the AID-Interface File is not present,
- or the AID-Interface File does not contain a record,
- or an error is detected in the TLV coding of an *AID-Interface Entry*,
- or a mandatory data object is missing in an *AID-Interface Entry*,
- or the coding of a data object in an *AID-Interface Entry* is not correct or inconsistent,

then the CPACE application shall discontinue processing the SELECT command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

The AID-Interface File shall be evaluated using the *AID* stored according to Req C.32.

Note:

The *AID* may be longer than the file name contained in the data field of the SELECT command.

The AID-Interface File shall be evaluated as follows:

- The CPACE application shall search for the first record of the AID-Interface File containing the *AID-Interface Entry* for which **both** of the following are true:
  - *AID* begins with the *DF-Name* in the *AID-Interface Entry*,
  - **and** the *Interface Descriptor* following *DF-Name* in the *AID-Interface Entry* indicates that the *AID-Interface Entry* is applicable to the interface in use.

  If such a record cannot be found in the AID-Interface File, then the CPACE application shall discontinue processing the SELECT command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

  If such a record is found, processing continues as follows with the *AID-Interface Entry* contained in this record.
- If the *GPO Parameters Reference Template* is absent from the *AID-Interface Entry*, then the default value '01' shall be used as *GPO Parameters Reference*.
- If the *GPO Parameters Reference Template* is present in the *AID-Interface Entry*, then the *GPO Parameters Reference* to be used for the transaction is retrieved from the *GPO Parameters Reference Template* according to the rules described for the cases a), b) and c) in the definition of the *AID-Interface Entry* (see Section 21.17).
- The *FCI Proprietary Template* data object (including tag and length) is retrieved from the *AID-Interface Entry*.

Req C.35 Build FCI

The FCI to be returned in the response data field for the SELECT command shall be built by encapsulating the concatenation of

- a *DF Name* data object
- and the *FCI Proprietary Template* data object retrieved according to Req C.34

in an *FCI* data object (tag '6F', correct length).

The *DF Name* in the value field of the *DF Name* data object shall be determined as follows:

If **both** of the following are true:

- the interface in use is contactless,
- and the file name received in the SELECT command data field is shorter than or equal to the *DF-Name* in the *AID-Interface Entry*,

then the *DF Name* in the *AID-Interface Entry* shall be used,

else *AID* shall be used.

Req C.36	**Blocked application**
If the application is blocked (i.e. 'Application Blocked' in *PTH* has the value 1b), then the CPACE application shall discontinue processing the SELECT command, and shall return a response message consisting of the *FCI* data object built according to Req C.35 and SW1 SW2 = '6283' (Selected file invalidated).	

If the application is not blocked, the following requirements apply.

Req C.37	**Store interface in use**
The CPACE application shall store transiently for further processing, which interface, contact or contactless, is used. If the Internal Data Logging implementer-option is supported, then • 'Interface' in *Environment in Use* shall be set to CONTACT, if the contact interface is used. • 'Interface' in *Environment in Use* shall be set to CONTACTLESS, if the contactless interface is used.	

Req C.38 Activate contactless access to card - SELECT

If **all** of the following are true:

- the Activation/Deactivation of Contactless Access to Dual Interface Cards implementer-option is supported,
- **and** the interface currently used is contact,
- **and** the currently selected CPACE application has the right to activate/deactivate contactless access to the card (see Req C.17),
- **and** implicit activation of contactless access to the CPACE card is enabled (see Req C.17),

then contactless access to the CPACE card shall be activated (see Req C.17).

If the Contactless Control - Card implementer-option is supported, which implies that that the Contactless Control - Application implementer-option is supported too, then this requirement shall be implemented as follows:

- 'Right of application to activate/deactivate contactless access to the card' in *Contactless Control - Application* shall be evaluated to check, whether the currently selected CPACE application has the right to activate/deactivate contactless access to the card, i.e. 'Right of application to activate/deactivate contactless access to the card' in *Contactless Control - Application* = ENABLED.
- 'Activation of contactless access to the card with SELECT of an application on the contact interface' in *Contactless Control - Card* shall be evaluated to check, whether implicit activation of contactless access to the CPACE card is enabled, i.e. 'Activation of contactless access to the card with SELECT of an application on the contact interface' in *Contactless Control - Card* = ENABLED.
- 'State of contactless access to the card' in *Contactless Control - Card* shall be used to activate contactless access to the CPACE card, i.e. 'State of contactless access to the card' in *Contactless Control - Card* shall be set to ACTIVATED.

Note:

If *Contactless Control - Application* is not present in the CPACE application or if *Contactless Control - Card* is not present in the CPACE card, then the CPACE application shall use the value '80' (see Section 16.7). In this case contactless access to the CPACE card will remain unchanged.

Req C.39	**Activate contactless access to application - SELECT**

If **all** of the following are true:

- the interface currently used is contact,
- **and** implicit activation of contactless access to the CPACE application is enabled (see Req C.11),

then contactless access to the CPACE application shall be activated.

If the Contactless Control - Application implementer-option is supported, then this requirement shall be implemented as follows:

- 'Activation of contactless access to the application with SELECT of the application on the contact interface' in *Contactless Control - Application* shall be evaluated to check, whether implicit activation of contactless access to the CPACE application is enabled, i.e. 'Activation of contactless access to the application with SELECT of the application on the contact interface' in *Contactless Control - Application* = ENABLED.
- 'State of contactless access to the application' in *Contactless Control - Application* shall be used to activate contactless access to the CPACE application, i.e. 'State of contactless access to the application' in *Contactless Control - Application* shall be set to ACTIVATED.

Note:

If *Contactless Control - Application* is not present in the CPACE application, then the CPACE application shall use the value '80' (see Section 16.7). In this case contactless access to the CPACE application will remain unchanged.

Req C.40	**Positive response to the SELECT command**

The CPACE application shall return a response message consisting of the *FCI* data object built according to Req C.35 and SW1 SW2 = '9000'.

7 Initiate Application Processing

7.1 Introduction

This section refers to Section 8 of [CPA]:

- A modification and additional requirements regarding Section 8.5.1.1 of [CPA] (Command Format Validation for the GET PROCESSING OPTIONS Command) are described in Section 7.2.1.
- An additional requirement regarding Section 8.5.2 of [CPA] (Processing of the GET PROCESSING OPTIONS Command) is described in Section 7.2.2.
- An additional requirement regarding Section 8.5.3.2 of [CPA] (Profile Selection File Processing) is described in detail in Section 7.2.3.
- Additional requirements regarding Section 8.5.4.1 of [CPA] (Profile Behaviour) are described in Section 7.2.4.
- Additional processing steps defined by this specification to be inserted as a new sub-section (Relay Resistance Protocol Preparation) of Section 8.5 of [CPA] between Section 8.5.4 (Profile Behaviour) and Section 8.5.5 (Respond to GET PROCESSING OPTIONS Command) are described in Section 7.2.5.

7.2 GET PROCESSING OPTIONS Command

7.2.1 Command Format Validation

The CPACE application shall support the Profile Selection Using Card Data implementer-option (see Req C.23) using the AID-Interface Table (see Req C.30). The *GPO Parameters Reference* has been retrieved during Application Selection (see Req C.34).

Therefore, the first paragraph and Req 8.2 in Section 8.5.1.1 of [CPA] are replaced with the following Req C.41.

Req C.41	**Retrieve *GPO Parameters x* from *GPO Parameters* Template**
GPO Parameters x with x = *GPO Parameters Reference* determined according to Req C.34 shall be retrieved from the *GPO Parameters* template.	

Req 8.5 in Section 8.5.1.1 of [CPA] is replaced with the following Req C.42.

Req C.42	**Check length and format of PDOL Related Data**

If **any** of the following is true:

- the PDOL Related Data do not consist of a correctly TLV coded data object with tag '83',
- **or** the value of the GPO Template Length in the (correctly coded) data object with tag '83' is not consistent with the length of the PDOL Related Data indicated in L_c,
- **or** the value of the GPO Template Length does not equal the value of the GPO Command Data Length parameter in the data element *GPO Parameters x* used for the transaction,

then the CPACE application shall discontinue processing the GET PROCESSING OPTIONS command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6700' (Wrong Length).

7.2.2 Processing

The following requirement is inserted between the first and second paragraph in Section 8.5.2 of [CPA].

Req C.43	**Check contactless access activated/deactivated - GPO**

If the interface currently used is contactless (see Req C.7), then the CPACE application shall check, whether contactless access to the CPACE application is deactivated (see Req C.8).

If the Contactless Control - Application implementer-option is supported, then 'State of contactless access to the application' in *Contactless Control - Application* shall be evaluated to check whether contactless access to the CPACE application is Deactivated, i.e. 'State of contactless access to the application' in *Contactless Control - Application* = DEACTIVATED.

If the Activation/Deactivation of Contactless Access to Dual Interface Cards implementer-option is supported and if the interface currently used is contactless (see Req C.7), then the CPACE application shall also check, whether contactless access to the CPACE card is deactivated (see Req C.13).

If the Contactless Control - Card implementer-option is supported, then 'State of contactless access to the card' in *Contactless Control - Card* shall be evaluated to check whether contactless access to the CPACE application is deactivated, i.e. 'State of contactless access to the Card' in *Contactless Control - Card* = DEACTIVATED.

If the interface currently used is contactless but contactless access to the CPACE application or to the CPACE card is deactivated, then the CPACE application shall discontinue processing the GET PROCESSING OPTIONS command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

Req 8.7 in Section 8.5.2 of [CPA] is replaced with the following Req C.44.

Req C.44	**Check *ATC* and reset transient transaction data**

If the value of the *ATC* is less than 'FFFF', then the application shall:

- increment the ATC by one,
- reset transient transaction data, such as:
  - reset the *Application Decisional Results (ADR)* to '00 00 00 00 00 00'
  - reset the *Card Verification Results (CVR)* to '00 00 00 00 00'
  - reset *Internal Flags* (if implemented) to zero
  - reset the *RRP Counter* to '00', if the Relay Resistance Protocol implementer-option is supported

Otherwise (the *ATC* has the value 'FF FF'), the application shall discontinue processing the GET PROCESSING OPTIONS command and respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

7.2.3 Profile Selection File Processing

Req 8.10 and 8.11 in Section 8.5.3.2 of [CPA] are replaced with the following requirement and text.

Req C.45	**Perform Profile Selection File Processing**

Profile Selection File Processing shall be performed as described in the remainder of this section.

Note:

If 'Allow Profile Selection with Extended Check Types' (byte 4, bit b2) in the *Application Control* has the value 0b, then Profile Selection File Processing described in this section is the same as Profile Selection File Processing described in Annex A of [CPA] taking into account error handling according Req 8.11 in Section 8.5.3.2 of [CPA].

According to this specification, Profile Selection may also use Extended Check Types providing a mechanism which uses the status of the accumulator(s) and counter(s) of the CPACE application for selecting a Profile by comparing of the current values of accumulator(s) or counter(s) with personalised data or with their respective limit(s).

In detail, the following additional tests using accumulators and counters of a CPACE application shall be supported for Profile Selection with Extended Check Types:

- Test whether *Accumulator x* is greater/less than a comparison value in the *Profile Selection Entry*.

- Test whether *Accumulator x* + Transaction Amount is greater/less than a comparison value in the *Profile Selection Entry* (only applicable if the transaction currency matches the accumulator currency).
- Test whether *Accumulator x* is greater/less than one of the *Accumulator x Limits*.
- Test whether *Accumulator x* + Transaction Amount is greater/less than one of the *Accumulator x Limits* (only applicable if the transaction currency matches the accumulator currency).
- Test whether *Counter x* is greater/less than a comparison value in the *Profile Selection Entry*.
- Test whether *Counter x* + 1 is greater/less than a comparison value in the *Profile Selection Entry*.
- Test whether *Counter x* is greater/less than one of the *Counter x Limits*.
- Test whether *Counter x* + 1 is greater/less than one of the *Counter x Limits*.

Note:

- The tests including the Transaction Amount are only applicable if the transaction currency matches the accumulator currency. No currency conversion is applied, even if currency conversion is supported for the respective Accumulator.
- For the tests including the Transaction Amount, the Transaction Amount and the Transaction Currency Code have to be present in and to be extracted from the GPO Input Data, i.e. the Transaction Amount and the Transaction Currency Code have to be requested by the PDOL.

Profile Selection using Extended Check Types can be used, for example, by a CPACE application to decide whether PIN verification has to be requested from a kernel during contactless transaction processing: If a CPACE application allows offline transactions without cardholder verification as long as the cumulate amount of these transactions does not exceed an upper limit, the CVM List passed to the terminal should contain a *Card Verification Results (CVR)* with No CVM Required as CVM. But if this limit would be exceeded by cumulating the transaction amount of the current transaction, the CVM List passed to the terminal should not allow No CVM Required as CVM anymore but should require either Offline PIN verification (if offline transactions with cardholder verification can still be allowed) or Online PIN verification (if offline transactions with cardholder verification cannot be allowed or Card Risk Management parameters need to be updated by the issuer).

If the *Application Control* is missing, then the CPACE application shall discontinue processing the GET PROCESSING OPTIONS command and shall respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

If 'Activate Profile Selection File' (byte 2, bit b4) in the *Application Control* has the value 0b, the issuer has not requested to perform Profile Selection File Processing. In this case the transaction shall be processed using the default *Profile ID* '01'.

Otherwise, the following steps shall be performed to determine the Profile to be used for the transaction.

If the Profile Selection File is missing in the CPACE application the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

The *Profile Selection Entries* in the records of the Profile Selection File shall be processed in the order in which the records they are stored in appear in the Profile Selection File. Processing starts with the first record.

If the Profile Selection File does not contain at least one record, the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

The Profile Selection Diversifier shall be retrieved from byte 2 of the *GPO Parameters x.* This 1-byte value shall be inserted at the beginning of the GPO Input Data. The resulting byte sequence is called **Extended GPO Input Data**.

A *Profile Selection Entry* shall be processed as follows:

1. If **any** of the following is true:
   - the length of the record of the Profile Selection File in which the *Profile Selection Entry* is stored is less than 7 bytes,
   - **or** the value of the Entry Length in byte 1 of a *Profile Selection Entry* is less than 6,
   - **or** according to the value of the Entry Length in byte 1 of a *Profile Selection Entry* the *Profile Selection Entry* is longer than the record of the Profile Selection File the *Profile Selection Entry* is stored in,

   the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

   If according to the Entry Length in byte 1 of a *Profile Selection Entry* the *Profile Selection Entry* is shorter than the record of the Profile Selection File the *Profile Selection Entry* is stored in, the trailing bytes at the end of the record shall be ignored.

2. The Position P in Extended GPO Input Data is retrieved from byte 2 of the *Profile Selection Entry*. The Length L of Extraction Block and/or Comparison Block is retrieved from byte 3 of the *Profile Selection Entry*. The Number n of Comparison Blocks is retrieved from byte 4 of the *Profile Selection Entry*.

   If **either** of the following is true:
   - the value of the Entry Length in byte 1 of the *Profile Selection Entry* is not equal to n*L+6,
   - or **both** of the following are true:
     - P is greater than 0 or n is greater than 0,
     - **and** L is equal to 0,

the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

3. The Check Type is retrieved from byte n*L+5 of the *Profile Selection Entry*.

   If **either** of the following is true:

   - **both** of the following are true:
     - the 'Extended Check Type' bit (bit b8) in the Check Type has the value 0b,
     - **and** the Check Type is greater than '02',
   - **or both** of the following are true:
     - the 'Allow Profile Selection with Extended Check Types' bit (byte 4, bit b2) in the *Application Control* has the value 0b,
     - **and** the 'Extended Check Type' bit (bit b8) in the Check Type has the value 1b

   the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

   If the 'Extended Check Type' bit (bit b8) in the Check Type has the value 0b, processing shall continue with step 4.

   If the 'Extended Check Type' bit (bit b8) and the 'Use Accumulator or Counter' bit (bit b7) in the Check Type have the value 1b, processing shall continue with step 7.

   If the 'Extended Check Type' bit (bit b8) in the Check Type has the value 1b and the 'Use Accumulator or Counter' bit (bit b7) in the Check Type has the value 0b, processing shall continue with step 8.

4. A value shall be extracted from the Extended GPO Input Data. The part to be extracted is defined using the two parameters P and L.

   If **either** of the following is true:

   - P is equal to 0,
   - **or** P and L would require extracting data beyond the length of the Extended GPO Input Data,

   the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

5. The extracted Value shall be masked with the Bit Mask to force some bits to 0. That is, for each bit in the Bit Mask that is set to the value 0, the corresponding bit in extracted value shall be set to 0.

   If n is less than 2, i.e. if the Comparison Blocks do not contain a Bit Mask, the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

6. The test indicated by the Check Type shall be performed as follows:

Match (Check Type = '00')

It shall be tested whether the masked value extracted from the Extended GPO Input Data is equal to any of the comparison value(s) in this *Profile Selection Entry*.

If a match is found, the Positive Action shall be performed.

If no match is found, the Negative Action shall be performed.

Less Than (Check Type = '01')

It shall be tested whether the masked value extracted from the Extended GPO Input Data is less than comparison value 1.

If the value of the masked extracted data is less than the value of comparison value 1, the Positive Action shall be performed.

If the value of the masked extracted data is greater than or equal to the value of comparison value 1, the Negative Action shall be performed.

Greater Than (Check Type = '02')

It shall be tested whether the masked value extracted from the Extended GPO Input Data is greater than comparison value 1.

If the value of the masked extracted data is greater than the value of comparison value 1, the Positive Action shall be performed.

If the value of the masked extracted data is less than or equal to the value of comparison value 1, the Negative Action shall be performed.

The Positive or Negative Action shall be evaluated as described in step 9.

7. If the 'Use Accumulator or Counter' bit (bit b7) in the Check Type has the value 1b indicating that an accumulator shall be used, the following steps shall be performed:

a) *Accumulator x* shall be retrieved from the *Accumulators Data* template, where x is the value of bits b6 and b5 of the Check Type.

If **any** of the following is true:

- the value x of bits b6 and b5 is 00b,
- **or** *Accumulator x* is missing in the *Accumulators Data* template,
- **or** *Accumulator x* does not have the format n 12,

the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

b) If the 'Add Transaction (Amount)' bit (bit b2) in the Check Type has the value 1b, the Transaction Amount shall be extracted from the Extended GPO Input Data. The part to be extracted is defined using the two parameters P and L.

If **any** of the following is true:

- P is equal to 0,
- **or** L is not equal to 6,
- **or** P and L would require extracting data beyond the length of the Extended GPO Input Data,
- **or** the 6-byte value extracted from the Extended GPO Input Data does not have the format n 12,

the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

Accumulator x and Transaction Amount are used to compute the value ***Temp Accumulator x***:

- If *Accumulator x* + Transaction Amount >= 10^{12}:

  Temp Accumulator x := 10^{12} - 1.

- Otherwise:

  Temp Accumulator x := *Accumulator x* + Transaction Amount.

c) n shall be evaluated to determine how to retrieve the **Comparison Value**.

If **either** of the following is true:

- n is greater than 1,
- **or both** of the following are true:
  - n is equal to 1,
  - **and either** of the following is true:
    - L is not equal to 6,
    - **or** the (only) 6-byte Comparison Block in the *Profile Selection Entry* does not have the format n 12,

the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

If n is equal to 1, the Comparison Value is the (only) 6-byte Comparison Block in the *Profile Selection Entry*.

If n is equal to 0, the Comparison Value is one of the *Accumulator x Limits* that shall be retrieved as follows:

- *Accumulator x Limits* shall be retrieved from the *Accumulators Data* template. The 'Limit Set ID' bit (bit b4) and the 'Lower/Upper Limit' bit (bit b3) in the Check Type shall be evaluated as described below in order to determine the Limit to be used:
  - If the 'Limit Set ID' bit has the value 0b, Limit Set 0 (bytes 1-12 in the *Accumulator x Limits*) shall be used.
  - If the 'Limit Set ID' bit has the value 1b, Limit Set 1 (bytes 13-24 in the *Accumulator x Limits*) shall be used.
  - If the 'Lower/Upper Limit' bit has the value 0b, the Lower Limit in the Limit Set identified by the 'Limit Set ID' bit shall be used.
  - If the 'Lower/Upper Limit' bit has the value 1b, the Upper Limit in the Limit Set identified by the 'Limit Set ID' bit shall be used.
- If **any** of the following is true:
  - *Accumulator x Limits* is missing in the *Accumulators Data* template,
  - **or both** of the following are true:
    - Accumulator x Lower/Upper Limit 1 shall be used,
    - **and** *Accumulator x Limits* has a length of 12 bytes,
  - **or** the Accumulator x Lower/Upper Limit to be used does not have the format n 12,

  the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

d) The test indicated by the 'Less/Greater Than' bit (bit b1) in the Check Type shall be performed as follows:

Less Than ('Less/Greater Than' bit = 0b)

It shall be tested whether *Accumulator x* or *Temp Accumulator x* is less than the Comparison Value.

If (*Temp*) *Accumulator x* is less than the Comparison Value, the Positive Action shall be performed.

If (*Temp*) *Accumulator x* is greater than or equal to the Comparison Value, the Negative Action shall be performed.

Greater Than ('Less/Greater Than' bit = 1b)

It shall be tested whether *Accumulator x* or *Temp Accumulator x* is greater than the Comparison Value.

If (*Temp*) *Accumulator x* is greater than the Comparison Value, the Positive Action shall be performed.

If (Temp) *Accumulator x* is less than or equal to the Comparison Value, the Negative Action shall be performed.

The Positive or Negative Action shall be evaluated as described in step 9.

8. If the 'Use Accumulator or Counter' bit (bit b7) in the Check Type has the value 0b indicating that a counter shall be used, the following steps shall be performed:

   a) *Counter x* shall be retrieved from the *Counters Data* template, where x is the value of bits b6 and b5 of the Check Type, 00b representing 4.

   If *Counter x* is missing in the *Counters Data* template, the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

   b) If the 'Add Transaction (Amount)' bit (bit b2) in the Check Type has the value 1b, the value ***Temp Counter x*** shall be computed:

   - If *Counter x* has the value 'FF':

     Temp Counter x := 'FF'

   - Otherwise:

     Temp Counter x := (*Counter x*) + 1

   c) n shall be evaluated to determine how to retrieve the **Comparison Value**.

   If **either** of the following is true:

   - n is greater than 1,
   - **or both** of the following are true:
     - n is equal to 1,
     - **and** L is not equal to 1,

   the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

If n is equal to 1, the Comparison Value is the (only) 1-byte Comparison Block in the *Profile Selection Entry*.

If n is equal to 0, the Comparison Value is one of the *Counter x Limits* that shall be retrieved as follows:

- *Counter x Limits* shall be retrieved from the *Counters Data* template. The 'Limit Set ID' bit (bit b4) and the 'Lower/Upper Limit' bit (bit b3) in the Check Type shall be evaluated as described below in order to determine the Limit to be used:
  - If the 'Limit Set ID' bit has the value 0b, Limit Set 0 (bytes 1-2 in the *Counter x Limits*) shall be used.
  - If the 'Limit Set ID' bit has the value 1b, Limit Set 1 (bytes 3-4 in the *Counter x Limits*) shall be used.
  - If the 'Lower/Upper Limit' bit has the value 0b, the Lower Limit in the Limit Set identified by the 'Limit Set ID' bit shall be used.
  - If the 'Lower/Upper Limit' bit has the value 1b, the Upper Limit in the Limit Set identified by the 'Limit Set ID' bit shall be used.
- If **either** of the following is true:
  - *Counter x Limits* is missing in the *Counters Data* template,
  - **or both** of the following are true:
    - Counter x Lower/Upper Limit 1 shall be used,
    - **and** *Counter x Limits* has a length of 2 bytes,

  the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

d) The test indicated by the 'Less/Greater Than' bit (bit b1) in the Check Type shall be performed as follows:

Less Than ('Less/Greater Than' bit = 0b)

It shall be tested whether *Counter x* or Temp *Counter x* is less than the Comparison Value.

If (*Temp*) *Counter x* is less than the Comparison Value, the Positive Action shall be performed.

If (*Temp*) *Counter x* is greater than or equal to the Comparison Value, the Negative Action shall be performed.

Greater Than ('Less/Greater Than' bit = 1b)

It shall be tested whether *Counter x* or Temp *Counter x* is greater than the Comparison Value.

If (*Temp*) *Counter x* is greater than the Comparison Value, the Positive Action shall be performed.

If (*Temp*) *Counter x* is less than or equal to the Comparison Value, the Negative Action shall be performed.

The Positive or Negative Action shall be evaluated as described in step 9.

9. The Positive or Negative Action shall be evaluated as follows:

- Bit b8 of the (Positive or Negative) Action byte has the value 0:

  If the value x of bits b7-b1 of the (Positive or Negative) Action byte is not equal to '00', then x shall be the *Profile ID* used for the transaction.

  Otherwise the *Profile ID* '7F' shall be used.

- Bit b8 of the (Positive or Negative) Action byte has the value 1b:

  If the value x of bits b7-b1 of the (Positive or Negative) Action byte is neither

  - equal to '00'
  - **nor** greater than RL - RC, where RC is the record number of the currently processed *Profile Selection Entry* and RL is the record number of the last record in the Profile Selection File

  then the profile selection algorithm shall move down x Profile Selection Entries, that is, to the *Profile Selection Entry* with the record number RC + x.

  Otherwise the process shall be terminated and the *Profile ID* used for the transaction shall be '7F'.

If the *Profile ID* determined by the Profile Selection processing is '7F', then the CPACE application shall discontinue processing the GET PROCESSING OPTIONS command and shall respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

Otherwise the *Profile Control* selected for the transaction shall be *Profile Control x*, where x is the value of the *Profile ID* selected for the transaction.

Note:

- If *Temp Accumulator x* and/or *Temp Counter x* are computed during Profile Selection, implementations should store these values transiently for Velocity Checking during first GENERATE AC processing, if this improves performance.
- If *Temp Accumulator x* is stored it has to be taken into account that for contact transactions the Transaction Amount sent in the command message of the first GENERATE AC command may differ from the Transaction Amount sent in the command message of the GET PROCESSING OPTIONS command. Therefore, if *Temp Accumulator x* is stored, the Transaction Amount should also be stored and

compared to the Transaction Amount sent in the first GENERATE AC command message before re-using *Temp Accumulator x*.

7.2.4 Profile Behaviour

The following requirement is inserted between Req 8.12 and the following paragraph in Section 8.5.4.1 of [CPA].

Req C.46	**Check *Profile Control x***

If 'Use Additional Accumulators and Counter' (byte 4, bit b3) in the *Application Control* has the value 0b, *Profile Control x* shall have a length of 8 bytes.

If 'Use Additional Accumulators and Counter' in the *Application Control* has the value 1b, *Profile Control x* shall have a length of 10 bytes.

If the length of *Profile Control x* is not correct, then the CPACE application shall discontinue processing the GET PROCESSING OPTIONS command and shall respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

If *Profile Control x* has a length of 8 bytes, it shall be padded implicitly with 2 trailing bytes 'FF' to a length of 10 bytes and it shall be used as *Profile Control* in the same way as a *Profile Control x* with a length of 10 bytes where bytes 9 and 10 have the value 'FF'.

In this way processing of the *Profile Control* will be the same irrespective of the value of 'Use Additional Accumulators and Counter' in the *Application Control*.

Note:

Setting bytes 9 and 10 of *Profile Control x* to the value 'FF' has the result, that Accumulator 3 and Counter 4 are not active for the transaction.

The following text and requirement are appended at the end of Section 8.5.4.1 of [CPA].

Preparatory steps for the Relay Resistance Protocol are performed during GET PROCESSING OPTIONS command processing (see Section 7.2.5), provided the Relay Resistance Protocol implementer-option is supported and the Relay Resistance Protocol shall be performed for the transaction.

Since a bit in the *Issuer Options Profile Control* indicates whether the Relay Resistance Protocol shall be performed for the transaction, selection of the *Issuer Options Profile Control* cannot be postponed until GENERATE AC processing but has to be performed during GET PROCESSING OPTIONS command processing if the Relay Resistance Protocol implementer-option is supported.

Req C.47	**Select *Issuer Options Profile Control* for the transaction**
If the Relay Resistance Protocol implementer-option is supported, *Issuer Options Profile Control* used in processing the transaction shall be selected and checked now, during GET PROCESSING OPTIONS command processing. The *Issuer Options Profile Control* used in processing the transaction shall be *Issuer Options Profile Control x*, where x is the Issuer Options Profile Control ID in the *Profile Control* for the transaction. If 'Allow Extended Controls' (byte 4, bit b1) in *Application Control* has the value 0b, the *Issuer Options Profile Control x* shall have a length of 7 bytes. If 'Allow Extended Controls' in *Application Control* has the value 1b, the *Issuer Options Profile Control x* shall have a length of 7 or 10 bytes. If the length of *Issuer Options Profile Control x* is not correct, then the CPACE application shall discontinue processing the GET PROCESSING OPTIONS command and shall respond with SW1 SW2 = '6985' (Conditions of use not satisfied). If *Issuer Options Profile Control x* has a length of 7 bytes, it shall be padded implicitly with 3 trailing bytes '00' to a length of 10 bytes and it shall be used as *Issuer Options Profile Control* in the same way as an *Issuer Options Profile Control x* with a length of 10 bytes where bytes 8 to 10 have the value '00'. In this way processing of the *Issuer Options Profile Control* will be the same irrespective of the value of 'Allow Extended Controls' in the *Application Control*.	

7.2.5 Relay Resistance Protocol Preparation

Processing described in this section is only to be performed if the Relay Resistance Protocol implementer-option is supported.

The time needed to process the EXCHANGE RELAY RESISTANCE DATA command must vary as little as possible, whenever the command is executed. Therefore, processing of the EXCHANGE RELAY RESISTANCE DATA command shall only require retrieving data from volatile memory or storing data in volatile memory.

Preparatory steps are necessary to make the data used for EXCHANGE RELAY RESISTANCE DATA command processing available in volatile memory. Such steps shall be performed during GET PROCESSING OPTIONS command processing, provided the Relay Resistance Protocol implementer-option is supported and the Relay Resistance Protocol shall be performed for the transaction according to the value of the 'Relay Resistance Protocol Supported' bit in the *Issuer Options Profile Control*.

Req C.48	**Check support of Relay Resistance Protocol**

If the 'Relay Resistance Protocol Supported' bit in the *Issuer Options Profile Control* has the value 1b, then processing shall continue according to Req C.49.

Otherwise, if the 'Relay Resistance Protocol Supported' bit in the *Issuer Options Profile Control* has the value 0b, then processing shall continue with responding to the GET PROCESSING OPTIONS command according to Section 8.5.5 of [CPA].

Req C.49	**Retrieve *RRP Configuration Data Set* for currently used interface**

If **any** of the following is true:

- the RRP Configuration File is missing in the CPACE application,
- **or** 'Interface' in *Environment in Use* does not have the value CONTACTLESS,
- **or** the RRP Configuration File does not contain at least one record,
- **or** the length of the first record of the RRP Configuration File is less than 6 bytes,

then an *RRP Configuration Data Set* cannot be retrieved for the currently used interface and processing shall continue with responding to the GET PROCESSING OPTIONS command according to Section 8.5.5 of [CPA].

Otherwise, the *RRP Configuration Data Set* to be used for contactless transactions shall be retrieved from the first six bytes of the first record of the RRP Configuration File and processing shall continue according to Req C.50.

Note:

Currently, the Relay Resistance Protocol is only performed for contactless transactions for which the *RRP Configuration Data Set* stored in the first record of the RRP Configuration File is used. Therefore, if the currently used interface is not the contactless interface, no *RRP Configuration Data Set* is retrieved and the Relay Resistance Protocol is not performed.

Req C.50	**Generate *RRP Dynamic Number* and initialise *RRP Transaction Data Set***

A 12-byte random number, the *RRP Dynamic Number* shall be generated and stored transiently for Relay Resistance Protocol processing.

Bytes 1 to 8 of the *RRP Transaction Data Set* shall be set to '00..00'.

Bytes 9 to 14 of the *RRP Transaction Data Set* shall be set to the value of the *RRP Configuration Data Set* which has been retrieved according to Req C.49.

The 'RRP Initialised' flag shall be set.

Processing shall continue with responding to the GET PROCESSING OPTIONS command according to Section 8.5.5 of [CPA]

8 Relay Resistance Timing Check

8.1 Introduction

If the Relay Resistance Protocol implementer-option is not supported, the CPACE application shall treat the EXCHANGE RELAY RESISTANCE DATA command as unknown according to Req 6.3 in Section 6.3 of [CPA].

If the Relay Resistance Protocol implementer-option is supported, the CPACE application shall support processing of the EXCHANGE RELAY RESISTANCE DATA command as described in this section.

During a contactless transaction, after Initiate Application Processing and before Read Application Data, the kernel performs the Relay Resistance Timing Check, if the Relay Resistance Protocol is supported by the kernel and by the CPACE application.

Note:

For the CPACE application, bit b1 in byte 2 of the *Application Interchange Profile (AIP)* indicates to the kernel that the CPACE application supports the Relay Resistance Protocol.

The kernel sends the EXCHANGE RELAY RESISTANCE DATA command to the CPACE application with a random number (*Terminal Relay Resistance Entropy*) contained in the data field. The CPACE application responds with a random number (*Device Relay Resistance Entropy*) and timing estimates (*Min Time For Processing Relay Resistance APDU*, *Max Time For Processing Relay Resistance APDU* and *Device Estimated Transmission Time For Relay Resistance R-APDU*).

If the timings determined by the kernel exceed the maximum limit computed, the kernel will try again. The kernel will attempt up to two retries of the EXCHANGE RELAY RESISTANCE DATA command.

Terminal Verification Results (TVR) are used to permit the kernel and the CPACE application to be configured through the *Terminal Action Codes* and the *Issuer Action Codes* to decline or send transactions online in the event that timings are outside the limits computed.

8.2 EXCHANGE RELAY RESISTANCE DATA Command

8.2.1 EXCHANGE RELAY RESISTANCE DATA Command Coding

The EXCHANGE RELAY RESISTANCE DATA command message is coded as follows:

Code	Value
CLA	'80'
INS	'EA'
P1	'00'
P2	'00'
Lc	'04'
Data	*Terminal Relay Resistance Entropy*
Le	'00'

Table 7: EXCHANGE RELAY RESISTANCE DATA Command Message

8.2.2 EXCHANGE RELAY RESISTANCE DATA Command Format Validation

Req C.51	**Check P1-P2 for ERRD command**
If the value of P1 or P2 is different from '00', then the CPACE application shall discontinue processing the command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6A86' (Incorrect Parameters, P1-P2).	

Req C.52	**Check Lc for ERRD command**
If the value of Lc is different from '04', then the CPACE application shall discontinue processing the command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6700' (Wrong Length).	

8.2.3 EXCHANGE RELAY RESISTANCE DATA Command Processing

Req C.53	**Check ERRD conditions**

If **all** of the following are true:

- the 'RRP Initialised' flag is set,
- **and** the value of *RRP Counter* is less than 3,
- **and** the 'Offline DDA Performed' bit in the *CVR* is not set

then processing shall continue according to Req C.54.

Otherwise, the CPACE application shall discontinue processing the command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

Req C.54	**Update transiently stored ERRD data**

The *RRP Counter* shall be incremented by 1.

Bytes 1 to 4 of the *RRP Transaction Data Set* shall be updated with the *Terminal Relay Resistance Entropy* retrieved from the ERRD command data field.

Bytes 5 to 8 of the *RRP Transaction Data Set* shall be updated with the following 4-byte portion of the *RRP Dynamic Number*:

byte [(*RRP Counter*-1)*4 + 1] to byte [*RRP Counter**4] of the *RRP Dynamic Number*

8.2.4 Respond to EXCHANGE RELAY RESISTANCE DATA Command

Req C.55	**Build ERRD response data**

The response data field of the EXCHANGE RELAY RESISTANCE DATA command has a length of 12 bytes and consists of a primitive data object with tag '80', length '0A' and a value field consisting of bytes 5 to 14 of the *RRP Transaction Data Set*.

The coding of the response data field of the EXCHANGE RELAY RESISTANCE DATA command is shown in Table 8.

Position	Value	Length (in bytes)	Format
Byte 1	'80'	1	b
Byte 2	'0A'	1	b
Bytes 5 - 8	*Device Relay Resistance Entropy*	4	b
Bytes 9 - 10	*Min Time For Processing Relay Resistance APDU*	2	b
Bytes 11 - 12	*Max Time For Processing Relay Resistance APDU*	2	b
Bytes 13 - 14	*Device Estimated Transmission Time For Relay Resistance R-APDU*	2	b

Table 8: EXCHANGE RELAY RESISTANCE DATA Response Data

Req C.56	**Return ERRD response**
The response to the EXCHANGE RELAY RESISTANCE DATA command returned by the CPACE application shall consist of the response data field built according to Req C.55 followed by SW1 SW2 = '9000'	

9 Read Application Data

9.1 Introduction

This section refers to Section 9 of [CPA]:

- Requirements previously contained in Section 9.5.3 of [CPA] and an additional requirement regarding Section 9.5.2 of [CPA] (Processing of the READ RECORD Command) are described in Section 9.2.1.
- The remaining text of Section 9.5.3 of [CPA] (Respond to READ RECORD Command) is modified according to Section 9.2.2.
- Modifications regarding Section 9.7.2 of [CPA] (Transaction Log File) are described in Section 9.3.1.
- Modifications regarding Section 9.7.3 of [CPA] (File Containing the Profile Selection Entries) are described in Section 9.3.2.
- New requirements regarding the AID-Interface File are described in Section 9.3.3.2.
- New requirements regarding the RRP Configuration File are described in Section 9.3.3.3.

9.2 READ RECORD Command

9.2.1 Processing

Section 9.5.2 of [CPA] is modified as follows.

A READ RECORD command is received for each record designated in the AFL sent to the terminal during Initiate Application Processing.

Req 9.3 (SFI not found):

If the referenced SFI cannot be found, then the card shall discontinue processing the READ RECORD command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6A82' (file not found).

Req 9.4 (Record not found):

If the referenced record cannot be found, then the card shall discontinue processing the READ RECORD command and respond with SW1 SW2 = '6A83' (record number does not exist).

Req C.57	**Check contactless access allowed - READ RECORD**
The CPACE application shall support a mechanism that allows the issuer to specify which records in the files which can be referenced by SFI from the application may not be read using the READ RECORD command on the contactless interface. For example it shall be possible to forbid reading the Cardholder Name on the contactless interface.	

If the interface currently used is contactless (see Req C.7), then the CPACE application shall check, whether the READ RECORD command tries to access a record that shall not be read on the contactless interface.

If the Contactless Command Access Controls implementer-option is supported, then the application shall retrieve *Contactless READ RECORD Access* from the *Contactless Command Access Controls* template to decide whether a record may be read on the contactless interface.

If *Contactless READ RECORD Access* is not present in the application, then all records may be read on the contactless interface.

If *Contactless READ RECORD Access* is present, but does not have a length of 1 + 3*n bytes, where n >= 1, then the record shall not be read on the contactless interface.

If *Contactless READ RECORD Access* is present and if its length is correct, then its entries shall be evaluated as follows using P1 and P2 from the READ RECORD command message, starting with the first entry of the *Contactless READ RECORD Access*:

If **all** of the following are true:

- the SFI in P2 is equal to the SFI in byte 1 of the entry,
- **and** the value of P1 is greater than or equal to the value of byte 2 of the entry,
- **and** the value of byte 3 of the entry is greater than or equal to the value of byte 2 of the entry,
- **and** the value of P1 is less than or equal to the value of byte 3 of the entry,

then:

- if byte 1 of the *Contactless READ RECORD Access* is '00' (positive access list), then the record may be read on the contactless interface,
- if byte 1 of the *Contactless READ RECORD Access* is '01' (negative access list), then the record shall not be read on the contactless interface,
- evaluation of the *Contactless READ RECORD Access* shall be terminated,

else:

- if there is another entry in the *Contactless READ RECORD Access*, then it shall be evaluated,
- if there is no other entry in the *Contactless READ RECORD Access*,

  then:

  - if byte 1 of the *Contactless READ RECORD Access* is '00' (positive access list), then the record shall not be read on the contactless interface,
  - if byte 1 of the *Contactless READ RECORD Access* is '01' (negative access list), then the record may be read on the contactless interface.

If the CPACE application receives a READ RECORD command on the contactless interface which tries to access a record that shall not be read on the contactless interface, then the CPACE application shall discontinue processing the command, shall respond with an SW1 SW2 that indicates an error and should use SW1 SW2 = '6985' (Conditions of use not satisfied).

The card receives each READ RECORD command from the terminal and returns the requested record to the terminal as described in Section 9.2.2 The terminal continues to issue READ RECORD commands until all designated records within each designated file have been read.

9.2.2 Respond to READ RECORD Command

The command response returned by the card includes the requested record in the data field.

For records in files with SFI in the range from 1 to 10, the data field of the response is formatted as described in EMV Book 3, section 6.5.11.4 (that is, with template tag '70', and TLV coded).

Note:

The READ RECORD command returns the record as stored in the file. Therefore records in files with SFI in the range from 1 to 10 have to be stored as TLV with record template tag '70'.

The card is allowed to send filler bytes of value '00' in the READ RECORD response for the Profile Selection file and for the AID-Interface File.

The format of records in files with SFI in the range from 11 to 30 other than the VLP Data file, the Transaction Log file, the Profile Selection file and the AID-Interface File is out of scope for this specification.

9.3 Additional File Requirements

9.3.1 Transaction Log File

The paragraph preceding Req 9.7 in Section 9.7.2 of [CPA] is replaced with the following text.

The CPACE application supports flexible logging of transaction data. The content of the Transaction Log records is the concatenation of the data element values constructed as described in Annex D of [CPA] and in Section 17 of this specification. The records in the Transaction Log file do not include a template tag.

The paragraph following Req 9.7 in Section 9.7.2 of [CPA] is replaced with the following text.

The conditions whether to log a transaction, and the content of the log are defined in Annex D of [CPA] and in Section 17 of this specification. Implementations may support more than ten records in the Transaction Log.

9.3.2 File Containing the Profile Selection Entries

Req 9.10 and the following paragraph in Section 9.7.3 of [CPA] are replaced with the following requirement and note.

Req C.58	**Minimum size of the Profile Selection File**
At a minimum, the CPACE application shall support up to 30 *Profile Selection Entries* in the Profile Selection File where each *Profile Selection Entry* may have, at a minimum, a length of up to 50 bytes.	

Note:

Implementations may support more than 30 *Profile Selection Entries*, and implementations may support *Profile Selection Entries* that are longer than 50 bytes.

If allowed by issuer implementation requirements, implementations may also support fewer than 30 *Profile Selection Entries*, or implementations may support *Profile Selection Entries* that are shorter than 50 bytes.

9.3.3 Additional Files of the CPACE Application

9.3.3.1 Introduction

In addition to the files defined in Section 9.7 of [CPA], the CPACE application shall support the AID-Interface File described in Section 9.3.3.2. If the Relay Resistance Protocol implementer-option is supported, the CPACE application shall also support the RRP Configuration File described in Section 9.3.3.3.

9.3.3.2 AID-Interface File

The AID-Interface File contains the *AID-Interface Entries*. Each record in the file contains one *AID-Interface Entry* without a record template tag.

Together, the records in the AID-Interface File are referred to as the AID-Interface Table.

Req C.59	**Minimum size of the AID-Interface Table**
At a minimum, the CPACE application shall support up to 16 *AID-Interface Entries* in the AID-Interface File where each *AID-Interface Entry* may have the maximum record length of 255 bytes.	

Note:

Implementations may support more than 16 *AID-Interface Entries* in the AID-Interface File.

If allowed by issuer implementation requirements, implementations may also support fewer than 16 *AID-Interface Entries* in the AID-Interface File or *AID-Interface Entries* with a maximum record length of less than 255 bytes.

Req C.60	**READ RECORD access to AID-Interface File**
The AID-Interface File shall be accessible using the READ RECORD command. Each record is a variable length entry containing an *AID-Interface Entry*. The *AID-Interface Entries* shall be returned in the response to READ RECORD for the AID-Interface File 'as is', i.e. the response to READ RECORD shall not include a record template tag.	

Note:

Devices that read the AID-Interface File use the *AID-Interface File Entry* data element to determine the location (SFI) and the number of records to read.

Req C.61	**SFI for AID-Interface File**
The SFI of the AID-Interface File shall be in the range from 21 to 30.	

Req C.62	**AID-Interface File not listed in AFL**
The AID-Interface File shall not be designated in the Application File Locator.	

9.3.3.3 RRP Configuration File

If the Relay Resistance Protocol implementer-option is supported and if the Relay Resistance Protocol shall be supported for one or more profile(s) of a CPACE application, then the RRP Configuration File shall be present in the CPACE application. The RRP Configuration File contains the *RRP Configuration Data Set*s. Each record in the file contains one *RRP Configuration Data Set* without a record template tag.

Req C.63	**Minimum size of the RRP Configuration File**
At a minimum, the CPACE application shall support one *RRP Configuration Data Set* in the RRP Configuration File where an *RRP Configuration Data Set* has a length of 6 bytes. An *RRP Configuration Data Set* may be shorter than the record of the RRP Configuration File in which the *RRP Configuration Data Set* is stored. In this case the *RRP Configuration Data Set* shall be stored left adjusted in the record with trailing filler bytes '00' at the end of the record.	

Note:

Implementations may support more than one *RRP Configuration Data Set* in the RRP Configuration File. But currently, the Relay Resistance Protocol is only performed for contactless transactions for which the *RRP Configuration Data Set* stored in the first record of the RRP Configuration File is used.

Req C.64	**READ RECORD access to RRP Configuration File**
The RRP Configuration File shall be accessible using the READ RECORD command. Each record contains an *RRP Configuration Data Set*, possibly followed by '00' filler bytes. The *RRP Configuration Data Set*s shall be returned in the response to READ RECORD for the RRP Configuration File 'as is', i.e. the response to READ RECORD shall not include a record template tag and shall include the trailing filler bytes, if present.	

Note:

Devices that read the RRP Configuration File use the *RRP Configuration File Entry* data element to determine the location (SFI) and the number of records to read.

Req C.65	**SFI for RRP Configuration File**
The SFI of the RRP Configuration File shall be in the range from 21 to 30.	

Req C.66	**RRP Configuration File not listed in AFL**
The RRP Configuration File shall not be designated in the Application File Locator.	

10 Offline Data Authentication

10.1 Introduction

This section refers to Section 10 of [CPA]:

An additional requirement regarding Section 10.7.1.2 of [CPA] (Processing of the INTERNAL AUTHENTICATE Command) is described in Section 10.2.

10.2 INTERNAL AUTHENTICATE Command

The following requirement is inserted at the beginning of Section 10.7.1.2 of [CPA].

Req C.67	**Check contactless access allowed - INTERNAL AUTHENTICATE**

The CPACE application shall support a mechanism that allows the issuer to specify whether the INTERNAL AUTHENTICATE command may be processed on the contactless interface or not.

If the interface currently used is contactless (see Req C.7), then the CPACE application shall check, whether the INTERNAL AUTHENTICATE command may be processed on the contactless interface.

If the Contactless Command Access Controls implementer-option is supported, then the application shall retrieve *Contactless Command Access* from the *Contactless Command Access Controls* template to decide whether the INTERNAL AUTHENTICATE command may be processed on the contactless interface.

If **either** of the following is true:

- *Contactless Command Access* is not present in the application,
- **or both** of the following are true:
  - *Contactless Command Access* is present in the application,
  - **and** 'INTERNAL AUTHENTICATE command on contactless interface' in *Contactless Command Access* = NOT ALLOWED,

then:

the INTERNAL AUTHENTICATE command shall not be processed on the contactless interface,

else:

the INTERNAL AUTHENTICATE command may be processed on the contactless interface.

Note:

If *Contactless Command Access* is present in the application, then it has a length of at least one byte. Additional length checks shall not be performed.

If the CPACE application receives the INTERNAL AUTHENTICATE command on the contactless interface, but the INTERNAL AUTHENTICATE command shall not be processed on the contactless interface, then the CPACE application shall discontinue processing the command, shall respond with an SW1 SW2 that indicates an error and should use SW1 SW2 = '6985' (Conditions of use not satisfied).

11 Cardholder Verification

11.1 Introduction

This section refers to Section 12 of [CPA]:

- A modification and an additional requirement regarding Section 12.5.2 of [CPA] (Processing of the GET DATA Command) are described in Section 11.2.
- An additional requirement regarding Section 12.6 of [CPA] (GET CHALLENGE Command) is described in Section 11.3.
- A modification regarding Section 12.7.1.1 of [CPA] (Command Format Validation for the VERIFY Command) is described in Section 11.4.1.
- Additional requirements regarding Section 12.7.2 of [CPA] (Processing of the VERIFY Command) are described in Section 11.4.2.

11.2 GET DATA Command

Req 12.6 in Section 12.5.1.1 of [CPA] is replaced with the following requirements.

Req C.68	**GET DATA support as described in EMV**
The CPACE application shall support the GET DATA command as described in Section 6.5.7 of [EMV 3] for retrieval of the data objects listed in Table J-1 in Annex J of [CPA] and in Table 40 in Section 19 that are supported by the GET DATA command.	

Req C.69	**Check contactless access allowed - GET DATA**
The CPACE application shall support a mechanism that allows the issuer to specify which data objects that are supported by the GET DATA command may not be read using the GET DATA command on the contactless interface. If the interface currently used is contactless (see Req C.7), then the CPACE application shall check, whether the GET DATA command tries to access a data object that shall not be read on the contactless interface. If the Contactless Command Access Controls implementer-option is supported, then the application shall retrieve *Contactless GET DATA Access* from the *Contactless Command Access Controls* template to decide whether a data object may be read on the contactless interface. If *Contactless GET DATA Access* is not present in the application, then all data objects may be read on the contactless interface. If *Contactless GET DATA Access* is present, but does not have a length of 1 + 2*n bytes, where n >= 1, then the data object shall not be read on the contactless interface.	

If *Contactless GET DATA Access* is present and if its length is correct, then its entries shall be evaluated as follows using P1 and P2 from the GET DATA command message, starting with the first entry of the *Contactless GET DATA Access*:

If P1 | P2 is equal to the entry,

then:

- if byte 1 of the *Contactless GET DATA Access* is '00' (positive access list), then the data object may be read on the contactless interface,
- if byte 1 of the *Contactless GET DATA Access* is '01' (negative access list), then the data object shall not be read on the contactless interface,
- evaluation of the *Contactless GET DATA Access* shall be terminated,

else:

- if there is another entry in the *Contactless GET DATA Access*, then it shall be evaluated,
- if there is no other entry in the *Contactless GET DATA Access*,
- then:
  - if byte 1 of the *Contactless GET DATA Access* is '00' (positive access list), then the data object shall not be read on the contactless interface,
  - if byte 1 of the *Contactless GET DATA Access* is '01' (negative access list), then the data object may be read on the contactless interface.

If the CPACE application receives a GET DATA command on the contactless interface which tries to access a data object that shall not be read on the contactless interface, then the CPACE application shall discontinue processing the command, shall respond with an SW1 SW2 that indicates an error and should use SW1 SW2 = '6985' (Conditions of use not satisfied).

11.3 GET CHALLENGE Command

The following requirement is inserted between the sub-heading "Challenge Computation" and the following paragraph in Section 12.6.2 of [CPA].

Req C.70	**Check contactless access allowed - GET CHALLENGE**

The CPACE application shall support a mechanism that allows the issuer to specify if the GET CHALLENGE command may be processed on the contactless interface or not.

If the interface currently used is contactless (see Req C.7), then the CPACE application shall check, whether the GET CHALLENGE command may be processed on the contactless interface.

If the Contactless Command Access Controls implementer-option is supported, then the application shall retrieve *Contactless Command Access* from the *Contactless Command Access Controls* template to decide as follows whether the GET CHALLENGE command may be processed on the contactless interface:

If **either** of the following is true:

- *Contactless Command Access* is not present in the application,
- **or both** of the following are true:
  - *Contactless Command Access* is present in the application,
  - **and** 'GET CHALLENGE command on contactless interface' in *Contactless Command Access* = NOT ALLOWED,

then:

the GET CHALLENGE command shall not be processed on the contactless interface,

else:

the GET CHALLENGE command may be processed on the contactless interface.

Note:

If *Contactless Command Access* is present in the application, then it has a length of at least one byte. Additional length checks shall not be performed.

If the CPACE application receives the GET CHALLENGE command on the contactless interface, but the GET CHALLENGE command shall not be processed on the contactless interface, then the CPACE application shall discontinue processing the command, shall respond with an SW1 SW2 that indicates an error and should use SW1 SW2 = '6985' (Conditions of use not satisfied).

11.4 VERIFY Command

11.4.1 Command Format Validation

Req 12.15 in Section 12.7.1.1 of [CPA] is replaced with the following requirement.

Req C.71	**Support for Offline Plaintext PIN in P2**
The CPACE application shall support the value '80' (Offline Plaintext PIN) in the P2 parameter for the VERIFY command only if the interface currently used is contact (see Req C.7). If the interface currently used is contactless, then the CPACE application shall not support the value '80' in the P2 parameter for the VERIFY command.	

11.4.2 Processing

The following requirement is inserted at the beginning of Section 12.7.2 of [CPA].

Req C.72	**Check contactless access allowed - VERIFY**

The CPACE application shall support a mechanism that allows the issuer to specify if the VERIFY command may be processed on the contactless interface or not.

If the interface currently used is contactless (see Req C.7), then the CPACE application shall check, whether the VERIFY command may be processed on the contactless interface.

If the Contactless Command Access Controls implementer-option is supported, then the application shall retrieve *Contactless Command Access* from the *Contactless Command Access Controls* template to decide as follows whether the VERIFY command may be processed on the contactless interface:

If **either** of the following is true:

- *Contactless Command Access* is not present in the application,
- **or both** of the following are true:
  - *Contactless Command Access* is present in the application,
  - **and** 'VERIFY command with Offline Enciphered PIN on contactless interface' in *Contactless Command Access* = NOT ALLOWED,

then:

the VERIFY command shall not be processed on the contactless interface,

else:

the VERIFY command may be processed on the contactless interface.

Note:

If *Contactless Command Access* is present in the application, then it has a length of at least one byte. Additional length checks shall not be performed.

If the CPACE application receives the VERIFY command on the contactless interface, but the VERIFY command shall not be processed on the contactless interface, then the CPACE application shall discontinue processing the command, shall respond with an SW1 SW2 that indicates an error and should use SW1 SW2 = '6985' (Conditions of use not satisfied).

The last part of Req 12.31 in Section 12.7.2.2 of [CPA] is changed as follows:

- If the recovered PIN matches the Reference PIN, then PIN verification is successful and the application shall:
  - set the 'Offline PIN Verification Performed and PIN Not Successfully Verified' bit in the *Card Verification Results (CVR)* to the value 0b.
  - reset the PIN Try Counter to the value of the PIN Try Limit.

- reset accumulators and counters according to Req C.73.
- activate contactless access to the CPACE card according to Req C.74.
- activate contactless access to the CPACE application according to Req C.75.
- indicate successful completion of the command by responding withSW1 SW2 = '9000'.

The following requirements are added at the end of Section 12.7.2.2 of [CPA].

Req C.73	**Reset accumulators and counters**

For all *Accumulator x*, for which **both** of the following are true:

- *Accumulator x* is active for the transaction,
- **and** 'Reset Accumulator with Offline PIN Verification' in the *Accumulator Profile Control* has the value 1b,

Accumulator x shall be accessed to be updated in the *Accumulators Data* template. If *Accumulator x* is not missing, it shall be updated with the value 0.

For all *Counter x*, for which **both** of the following are true:

- *Counter x* is active for the transaction,
- **and** 'Reset Counter with Offline PIN Verification' in the *Counter Profile Control* has the value 1b,

Counter x shall be accessed in the *Counters Data* template. If *Counter x* is not missing, it shall be updated with the value 0.

Req C.74 Activate contactless access to card - VERIFY

If **all** of the following are true:

- The Contactless Control - Card implementer-option is supported,
- **and** the interface currently used is contact,
- **and** 'Right of application to activate/deactivate contactless access to the card' in *Contactless Control - Application* = ENABLED,
- **and** 'Activation of contactless access to the card with successful VERIFY command on the contact interface' in *Contactless Control - Card* = ENABLED,

then contactless access to the CPACE card shall be activated and the (re-)deactivation mechanism for the card described in Req C.18 shall be disabled as follows:

- 'State of contactless access to the Card' in *Contactless Control - Card* shall be set to ACTIVATED,
- 'Enablement of unsecured DEACTIVATE CL command for the card' in *Contactless Control - Card* shall be set to DISABLED.

Note:

If *Contactless Control - Application* is not present in the CPACE application or if *Contactless Control - Card* is not present in the CPACE card, then the CPACE application shall use the value '80' (see Section 16.7). In this case contactless access to the CPACE card will remain unchanged.

Req C.75 Activate contactless access to application - VERIFY

If **all** of the following are true:

- The Contactless Control - Application implementer-option is supported,
- **and** the interface currently used is contact,
- **and** 'Activation of contactless access to the application with successful VERIFY command on the contact interface' in *Contactless Control - Application* = ENABLED,

then contactless access to the CPACE application shall be activated and the (re-)deactivation mechanism for the application described in Req C.12 shall be disabled as follows:

- 'State of contactless access to the application' in *Contactless Control - Application* shall be set to ACTIVATED,
- 'Enablement of unsecured DEACTIVATE CL command for the application' in *Contactless Control - Application* shall be set to DISABLED.

Note:

If *Contactless Control - Application* is not present in the CPACE application, then the CPACE application shall use the value '80' (see Section 16.7). In this case contactless access to the CPACE application will remain unchanged.

12 First Card Action Analysis

12.1 Introduction

This section refers to Section 15 of [CPA]:

- A modification and an additional requirement regarding Section 15.5.1.1 of [CPA] (Command Format Validation) are described in Section 12.2.1.
- Additional requirements regarding Section 15.5.2 of [CPA] (Profile Behaviour) are described in Section 12.2.2.
- Modifications regarding Section 15.5.3.4 of [CPA] (Terminal Erroneously Considers Offline PIN OK Check) are described in Section 12.2.3.1.
- Modifications and additional requirements regarding Sections 15.5.3.15, 15.5.3.16, 15.5.3.17 and 15.5.3.18 of [CPA] (Accumulator x and Counter x Velocity Checking) are described in Section 12.2.3.2.
- Additional Card Risk Management checks (Cashback Check and RRP Check) defined by this specification are described in Sections 12.2.3.3 and 12.2.3.4.
- A note and an additional requirement are added in Section 15.5.4 of [CPA] (Determine Response Application Cryptogram Type) as described in Section 12.2.4.
- Modifications regarding Section 15.5.5 of [CPA] (Application Approves Transaction Offline) are described in Section 12.2.5.
- Modifications and additional requirements regarding Section 15.5.6 of [CPA] (Application Requests Online Processing) are described in Section 12.2.6.
- Additional requirements regarding Section 15.5.8.1 of [CPA] (Build Issuer Application Data) are described in Section 12.2.7.1.
- A modification regarding Section 15.5.8.3 of [CPA] (Log Transactions for the First GENERATE AC Command) is described in Section 12.2.7.2.
- Additional processing steps defined by this specification (Store Transaction Data) to be inserted between Log Transaction and Return GENERATE AC Response are described in Section 12.2.7.3.
- Modifications and additional requirements regarding Section 15.5.8.4 of [CPA] (Return GENERATE AC Response) are described in Section 12.2.7.4.

12.2 First GENERATE AC Command

12.2.1 Command Format Validation

Req 15.5 in Section 15.5.1.1 of [CPA] is replaced with the following requirement.

Req C.76	**Check *Issuer Options Profile Control x***

If the Relay Resistance Protocol implementer-option is not supported, *Issuer Options Profile Control* used in processing the transaction shall be selected and checked now, during first GENERATE AC command processing.

The *Issuer Options Profile Control* used in processing the transaction shall be *Issuer Options Profile Control x*, where x is the Issuer Options Profile Control ID in the *Profile Control* for the transaction.

If 'Allow Extended Controls' (byte 4, bit b1) in *Application Control* has the value 0b, the *Issuer Options Profile Control x* shall have a length of 7 bytes.

If 'Allow Extended Controls' in *Application Control* has the value 1b, the *Issuer Options Profile Control x* shall have a length of 7 or 10 bytes.

If the length of *Issuer Options Profile Control x* is not correct, then the CPACE application shall discontinue processing the first GENERATE AC command and shall respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

If *Issuer Options Profile Control x* has a length of 7 bytes, it shall be padded implicitly with 3 trailing bytes '00' to a length of 10 bytes and it shall be used in the same way as an *Issuer Options Profile Control x* with a length of 10 bytes where bytes 8 to 10 have the value '00'.

In this way processing of *Issuer Options Profile Control x* will be the same irrespective of the value of 'Allow Extended Controls' in *Application Control*.

12.2.2 Profile Behaviour

The following requirement is inserted between the second note and Req 15.8 in Section 15.5.2 of [CPA].

Req C.77	**Determination of master keys to be used for the transaction**

If **either** of the following is true:

- the Additional Master Keys implementer-option is not supported,
- **or both** of the following are true:
  - the Additional Master Keys implementer-option is supported
  - **and** 'Master Keys ID' (bits b8-b5 of byte 7) in the *Profile Control* has the value '0',

then *Standard Master Keys*, i.e. the standard set of symmetric master keys defined in [CPA], shall be used for the transaction.

If **both** of the following are true:

- the Additional Master Keys implementer-option is supported,
- **and** 'Master Keys ID' (bits b8-b5 of byte 7) in the *Profile Control* has a value different from '0',

then *Additional Master Keys x*, where x has the value of 'Master Keys ID', shall be used for the transaction.

If the Cryptogram Version '5'-only implementer-option is supported, the master keys to be used for the transaction is a set of Triple DES keys, each with a length of 16 bytes.

If the Cryptogram Version '6'-only implementer-option is supported, the master keys to be used for the transaction is a set of AES keys each with the same length of either 16, 24 or 32 bytes.

If the Cryptogram Version '5' and '6' implementer-option is supported, the master keys to be used for the transaction is either a set of Triple DES keys, each with a length of 16 bytes, or a set of AES keys each with the same length of either 16, 24 or 32 bytes.

According to Specification Bulletin 165, the cryptographic algorithm to be used shall be indicated in the Profile CCI in the *Issuer Options Profile Control*. If the value of the Profile CCI in the *Issuer Options Profile Control* does not indicate the cryptographic algorithm assigned to the master keys to be used for the transaction, then the CPACE application shall discontinue processing the first GENERATE AC command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

The following requirement is inserted between Req 15.10 and Req 15.11 in Section 15.5.2 of [CPA].

Req C.78	**Check *Accumulator x Control* and *Accumulator Profile Control y***

For each *Accumulator x* that is active for the transaction with *Accumulator Profile Control y*, *Accumulator x Control* and *Accumulator Profile Control y* shall be checked as described below.

If 'Allow Extended Controls' (byte 4, bit b1) in *Application Control* has the value 0b, *Accumulator x Control* shall have a length of 3 bytes and *Accumulator Profile Control y* shall have a length of 2 bytes.

If 'Allow Extended Controls' in *Application Control* has the value 1b, *Accumulator x Control* shall have a length of 3 or 4 bytes and *Accumulator Profile Control y* shall have a length of 2 or 3 bytes.

If the length of *Accumulator x Control* or *Accumulator Profile Control y* is not correct, then Accumulator x is not (no longer) active for the transaction and the following steps shall be performed:

- 'Check Failed' (byte 5, bit b5) in the *Application Decisional Results (ADR)* shall be set to 1b,
- 'Check Failed' (byte 3, bit b2) in the *Card Verification Results (CVR)* shall be set to 1b.

If *Accumulator x Control* has a length of 3 bytes, it shall be padded implicitly with 1 trailing byte '00' to a length of 4 bytes and it shall be used in the same way as an *Accumulator x Control* with a length of 4 bytes where byte 4 has the value '00'.

If *Accumulator Profile Control y* has a length of 2 bytes, it shall be padded implicitly with 1 trailing byte '00' to a length of 3 bytes and it shall be used in the same way as an *Accumulator Profile Control y* with a length of 3 bytes where byte 3 has the value '00'.

In this way processing of *Accumulator x Control* and *Accumulator Profile Control y* will be the same irrespective of the value of 'Allow Extended Controls' in *Application Control*.

The following requirement is inserted between Req 15.13 and Req 15.14 in Section 15.5.2 of [CPA].

Req C.79	**Check *Counter x Control* and *Counter Profile Control y***

For each *Counter x* that is active for the transaction with *Counter Profile Control y*, *Counter x Control* and *Counter Profile Control y* shall be checked as described below.

If 'Allow Extended Controls' (byte 4, bit b1) in *Application Control* has the value 0b, *Counter x Control* and *Counter Profile Control y* shall have a length of 1 byte.

If 'Allow Extended Controls' in *Application Control* has the value 1b, *Counter x Control* and *Counter Profile Control y* shall have a length of 1 or 2 bytes.

If the length of *Counter x Control* or *Counter Profile Control y* is not correct, then Counter x is not (no longer) active for the transaction and the following steps shall be performed:

- 'Check Failed' (byte 5, bit b5) in the *Application Decisional Results (ADR)* shall be set to 1b,
- 'Check Failed' (byte 3, bit b2) in the *Card Verification Results (CVR)* shall be set to 1b.

If *Counter x Control* or *Counter Profile Control y* has a length of 1 byte, it shall be padded implicitly with 1 trailing byte '00' to a length of 2 bytes and it shall be used in the same way as an *Counter x Control* and *Counter Profile Control y* with a length of 2 bytes where byte 2 has the value '00'.

In this way processing of *Counter x Control* and *Counter Profile Control y* will be the same irrespective of the value of 'Allow Extended Controls' in *Application Control*.

12.2.3 Card Risk Management

12.2.3.1 Terminal Erroneously Considers Offline PIN OK Check

The first paragraph in Section 15.5.3.4 is replaced with the following text.

This mandatory check determines whether the terminal considers (in *CVM Results*) that Offline PIN processing passed, when the card reported Offline PIN processing as having failed. This information is considered, when deciding whether to approve or decline the transaction offline, or to send the transaction online. The issuer gets notification of this check, if 'Use Issuer Discretionary Bits in CVR' (byte 7, bit b5) in the *Issuer Options Profile Control* has the value 1b.

The last two paragraphs of Req 15.29 in Section 15.5.3.4 are replaced with the following text.

then the following steps shall be performed:

- 'Terminal Erroneously Considers Offline PIN OK' in the *Application Decisional Results (ADR)* (byte 2, bit b7) shall be set to 1b,
- if 'Use Issuer Discretionary Bits in CVR' (byte 7, bit b5) in the *Issuer Options Profile Control* has the value 1b, then 'Terminal Erroneously Considers Offline PIN OK' in the *Card Verification Results (CVR)* (byte 3, bit b3) shall be set to 1b.

12.2.3.2 Accumulator x and Counter x Velocity Checking

According to this specification, the functionality of Velocity Checking for *Accumulator x* and *Counter x* described in [CPA] has been extended to support accumulation and counting based on the *Transaction CVM*. In particular, the Transaction CVM check has been added to

decide whether a transaction amount may be accumulated in *Accumulator x* or whether a transaction may be counted in *Counter x*. This additional functionality is controlled by the fourth byte of *Accumulator x Control* and by the second byte of *Counter x Control*.

The Transaction CVM check, i.e. the check whether the *Transaction CVM* is (one of) the CVM(s) allowing accumulation or counting shall be performed as described in Req C.80 and Req C.81.

The following condition is inserted between the first and second condition of Req 15.41 and of Req 15.43 and between the second and third row of Table 15-7 in [CPA].

- the 'Allow Accumulation' bit in the *Accumulator Profile Control* for *Accumulator x* in this profile has the value 1b
- **and** the Transaction CVM is (one of) the CVM(s) allowing accumulation,
- **and** the 'Include Offline Approvals' bit in the *Accumulator x Control* has the value 1b,

The following condition is inserted between the first and second condition of Req 15.45 and of Req 15.47 in [CPA].

- the 'Allow Counting' bit in the *Counter Profile Control* for *Counter x* in this profile has the value 1b
- **and** the Transaction CVM is (one of) the CVM(s) allowing counting,
- **and** the 'Include Offline Approvals' bit in the *Counter x Control* has the value 1b,

Req C.80	**Determine *Transaction CVM***

The *Transaction CVM* shall be determined as follows:

- The *Transaction CVM* is Offline PIN if **both** of the following are true:
  - 'Offline PIN Verification Performed' (byte 2, bit b4) in the *Card Verification Results (CVR)* has the value 1b,
  - **and** 'Offline PIN Verification Performed and PIN Not Successfully Verified' (byte 2, bit b3) in the *Card Verification Results (CVR)* has the value 0b.

- If the *Transaction CVM* is not Offline PIN, i.e. if **either** of the following is true:
  - 'Offline PIN Verification Performed' in the *Card Verification Results (CVR)* has the value 0b,
  - **or** 'Offline PIN Verification Performed and PIN Not Successfully Verified' in the *Card Verification Results (CVR)* has the value 1b.

  then the *CVM Results*, retrieved from bytes 31-33 of the first GENERATE AC command data, shall be evaluated to determine the *Transaction CVM* as follows:
- The *Transaction CVM* is Online PIN if **both** of the following are true:
  - bits b6-b1 of byte 1 of the CVM Results have the value 000010b,
  - **and** byte 3 of the CVM Results has the value '00'.
- The *Transaction CVM* is Signature if **both** of the following are true:
  - bits b6-b1 of byte 1 of the CVM Results have the value 011110b,
  - **and** byte 3 of the CVM Results has the value '00'.
- If the *Transaction CVM* is neither Offline PIN nor Online PIN nor Signature according to the description above, the *Transaction CVM* is No CVM.

Req C.81	**Check whether *Transaction CVM* is (one of) the CVM(s) allowing accumulation or counting**

The *Transaction CVM* is (one of) the CVM(s) allowing accumulation if **any** of the following is true:

- the *Transaction CVM* is Offline PIN and 'Include if Transaction CVM is Offline PIN' (byte 4, bit b4) in the *Accumulator x Control* has the value 0b,
- **or** the *Transaction CVM* is Online PIN and 'Include if Transaction CVM is Online PIN' (byte 4, bit b3) in the *Accumulator x Control* has the value 0b,
- **or** the *Transaction CVM* is Signature and 'Include if Transaction CVM is Signature' (byte 4, bit b2) in the *Accumulator x Control* has the value 0b,
- **or** the *Transaction CVM* is No CVM and 'Include if Transaction CVM is No CVM' (byte 4, bit b1) in the *Accumulator x Control* has the value 0b.

The *Transaction CVM* is (one of) the CVM(s) allowing counting if **any** of the following is true:

- the *Transaction CVM* is Offline PIN and 'Include if Transaction CVM is Offline PIN' (byte 2, bit b4) in the *Counter x Control* has the value 0b,
- **or** the *Transaction CVM* is Online PIN and 'Include if Transaction CVM is Online PIN' (byte 2, bit b3) in the *Counter x Control* has the value 0b,
- **or** the *Transaction CVM* is Signature and 'Include if Transaction CVM is Signature' (byte 2, bit b2) in the *Counter x Control* has the value 0b,
- **or** the *Transaction CVM* is No CVM and 'Include if Transaction CVM is No CVM' (byte 2, bit b1) in the *Counter x Control* has the value 0b.

Note:

According to these rules, the value 0000b of bits b4-b1 of byte 4 in the *Accumulator x Control* and of bits b4-b1 of byte 2 in the *Counter x Control* indicates that accumulation or counting shall be performed irrespective of the *Transaction CVM*, that is, irrespective of whether and how cardholder verification was performed during the current transaction.

12.2.3.3 Cashback Check

This issuer-optional check is defined by this specification. It identifies whether the current transaction is a transaction with cashback. This information is considered, when deciding whether to approve or decline the transaction offline, or to send the transaction online.

Req C.82	**Check whether to perform Cashback Check**

The Cashback Check shall be performed, if and only if **all** of the following are true:

- 'Activate Cashback Check' (byte 7, bit b2) in the *Issuer Options Profile Control* has the value 1b,
- **and** a TC or an ARQC was requested in the first GENERATE AC command,
- **and** the CPACE application is not blocked.

If an AAC was requested in the first GENERATE AC command, or if an AAC has to be returned in the response message of the first GENERATE AC command because the application is blocked, processing of the Cashback Check shall be terminated.

Otherwise, processing of the Cashback Check shall continue according to the following requirement.

Req C.83	**Set 'Transaction with Cashback' bit in *ADR***
The 6-byte value Cashback Amount of the current transaction (Amount, Other) shall be retrieved from bytes 7-12 of the first GENERATE AC command data. The format of the 6-byte value Cashback Amount shall not be checked. If the Cashback Amount is greater than 0, the 'Transaction with Cashback' bit (byte 6, bit b8) in the *Application Decisional Results (ADR)* shall be set to 1b.	

12.2.3.4 RRP Check

The RRP Check is defined by this specification. This check is mandatory if the Relay Resistance Protocol implementer-option is supported. It requests a decline of the transaction if either of the following is true:

- The terminal considers the Relay Resistance Protocol not being performed though the EXCHANGE RELAY RESISTANCE DATA command was processed successfully by the CPACE application.
- The *Unpredictable Number* sent in the first GENERATE AC command data is different from the *Terminal Relay Resistance Entropy* sent in the EXCHANGE RELAY RESISTANCE DATA command data.

In addition, this check identifies whether CDA processing is requested by the terminal if the EXCHANGE RELAY RESISTANCE DATA command was processed successfully by the CPACE application. This information is considered, when deciding whether to approve or decline the transaction offline, or to send the transaction online.

Req C.84	**Check whether to perform the RRP Check**
The RRP Check shall be performed, if and only if **both** of the following are true: • The Relay Resistance Protocol implementer-option is supported, • **and** *RRP Counter* > 0, i.e. the EXCHANGE RELAY RESISTANCE DATA command was processed successfully by the CPACE application.	

If the Relay Resistance Protocol implementer-option is not supported, or if the EXCHANGE RELAY RESISTANCE DATA command was not processed successfully by the CPACE application, processing of the RRP Check shall be terminated.

Otherwise, processing of the RRP Check shall continue according to the following requirements.

Req C.85	**Set 'RRP Fatal Error' flag**

If **either** of the following is true:

- the 'Relay Resistance Protocol performed' bit (byte 5, bits b2 and b1) in the *TVR* sent in the first GENERATE AC command data has a value different from 10b (RRP performed),
- or the *Unpredictable Number* sent in the first GENERATE AC command data is different from the *Terminal Relay Resistance Entropy* stored in bytes 1 to 4 of *RRP Transaction Data Set*, i.e. sent in the EXCHANGE RELAY RESISTANCE DATA command data,

then the 'RRP Fatal Error' flag shall be set.

Req C.86	**Set 'RRP without CDA' bit in *ADR***

If the 'CDA Requested' bit in the P1 parameter in the GENERATE AC command message is 0b, i.e. CDA was not requested by the terminal, then the 'RRP without CDA' bit (byte 6, bit b7) in the *Application Decisional Results (ADR)* shall be set to 1b.

12.2.4 Determine Response Application Cryptogram Type

The following note and requirement are inserted between Req 15.60 and Req 15.61 in Section 15.5.4 of [CPA]:

Note:

If the 'Application Blocked' bit in the *PTH* has the value 1b an AAC shall be generated, irrespective of the AID with which the CPACE application was selected when this bit was set, even if that AID is different from the *AID* with which the CPACE application is currently selected.

Req C.87	**Decline transaction offline if 'RRP Fatal Error' flag is set**

If the 'RRP Fatal Error' flag is set, then an AAC type Application Cryptogram response to the first GENERATE AC shall be generated.

12.2.5 Application Approves Transaction Offline

According to this specification, the functionality of Velocity Checking for *Accumulator x* and *Counter x* described in [CPA] has been extended to support accumulation and counting based on the *Transaction CVM*. The Transaction CVM check, i.e. the check whether the *Transaction CVM* is (one of) the CVM(s) allowing accumulation or counting shall be performed as described in Req C.80 and Req C.81.

The first bulleted paragraph in Req 15.63 in Section 15.5.5 of [CPA] is replaced by the following paragraph.

- For each *Accumulator x* that is active for the transaction **and** the 'Include Offline Approvals' bit in the *Accumulator x Control* has the value 1b **and** the 'Allow Accumulation' bit in the *Accumulator Profile Control* for *Accumulator x* for this profile has the value 1b **and** the *Transaction CVM* is (one of) the CVM(s) allowing accumulation:

The first bulleted paragraph in Req 15.64 in Section 15.5.5 of [CPA] is replaced by the following paragraph.

- For each *Counter x* that is active for the transaction **and** the 'Allow Counting' bit in the *Counter Profile Control* for *Accumulator x* for this profile has the value 1b **and** the *Transaction CVM* is (one of) the CVM(s) allowing accumulation:

The condition regarding accumulation in Req 15.64 in Section 15.5.5 of [CPA] is replaced by the following condition.

- **and either** of the following is true:
  - the 'Include Only If Not Accumulated' bit in the *Counter x Control* has the value 0b,
  - **or** for all *Accumulators x*, which are active for the transaction,
    - 'Allow Accumulation' in the *Accumulator x Profile Control* has the value 0b,
    - **or** the *Transaction CVM* is not (one of) the CVM(s) allowing accumulation,
    - **or** 'Include Offline Approvals' (byte 3, bit b7) in the *Accumulator x Control* has the value 0b,
    - **or both** of the following are true:
      - the transaction currency does not match the accumulator currency,
      - **and** the transaction currency cannot be converted to the accumulator currency.

12.2.6 Application Requests Online Processing

According to this specification, the functionality described in [CPA] has been extended to support accumulation and counting of transactions which are authorised online.

Therefore, also if an ARQC shall be sent in the response to the first GENERATE AC command, accumulators and counters shall be updated as described below if this is required by the value of the (fourth byte of) *Accumulator x Control* and/or by the (second byte of) *Counter x Control*.

If an *Accumulator x* or a *Counter x* is updated according to this description, also the indicators in the *Card Verification Results (CVR)* for exceeding the respective limits shall be checked and, if necessary, updated.

The first paragraph in Section 15.5.6 of [CPA] is replaced with the following text and requirements.

The transaction is to go online for authorisation, if an ARQC type *Application Cryptogram* shall be sent in the response to the first GENERATE AC command. If this is the case,

- accumulators and counters,
- *Card Verification Results (CVR)*,
- *Cryptogram Information Data (CID)*,
- *Previous Transaction History (PTH)*

shall be updated as described in this section.

Req C.88	**Update accumulators and *CVR* for online request**

For each value of x for which **all** of the following are true:

- *Accumulator x* is active for the transaction,
- **and** 'Include Online Requests' (byte 4, bit b8) in the *Accumulator x Control* has the value 1b,
- **and** 'Allow Accumulation' (byte 1, bit b8) in the *Accumulator x Profile Control* has the value 1b,
- **and** the *Transaction CVM* is (one of) the CVM(s) allowing accumulation,
- **and either** of the following is true:
  - the transaction currency matches the accumulator currency,
  - **or** the transaction currency can be converted to the accumulator currency,

Accumulator x can be accumulated. In this case *Accumulator x* shall be updated in the *Accumulators Data* template as described below.

- If the transaction currency matches the accumulator currency:
  - If *Accumulator x* + Transaction Amount is (would be) greater than 10^{12} - 1,

    Accumulator x shall be updated with the value 10^{12} - 1.
  - Otherwise,

    Accumulator x shall be updated with

    Accumulator x + Transaction Amount.
- If the transaction currency does not match the accumulator currency (in which case the transaction currency can be converted to the accumulator currency, since Accumulator x is eligible for accumulation), the Transaction Amount shall be converted to the Converted Transaction Amount in accumulator currency.
  - If the Converted Transaction Amount or *Accumulator x* + Converted Transaction Amount is (would be) greater than 10^{12} - 1,

    Accumulator x shall be updated with the value 10^{12} - 1.
  - Otherwise,

    Accumulator x shall be updated with

    Accumulator x + Converted Transaction Amount.

If the new value of *Accumulator x* is greater than the Accumulator x Lower (Upper) Limit, 'Lower (Upper) Cumulative Offline Amount Limit Exceeded' (byte 3, bit b6 (b5)) in the *Card Verification Results (CVR)* shall be set to 1b.

Note:

- If *Accumulator x* is also eligible for offline accumulation, i.e. if 'Include Offline Approvals' (byte 3, bit b7) in the *Accumulator x Control* has the value 1b, and if **either** of the following is true:
  - a TC was requested in the first GENERATE AC command,
  - **or both** of the following are true:
    - an ARQC was requested in the first GENERATE AC command,
    - **and** 'Include ARQC Transaction in CRM Test' (byte 3, bit b8) in the *Accumulator x Control* has the value 1b,

  Temp Accumulator x, that is *Accumulator x* + Transaction Amount, has already been computed during Cumulating Velocity Checking as described in Sections 15.5.3.15 and 15.5.3.16 of [CPA] and shall not be computed again.
- If the (Converted) Transaction Amount is equal to 0 or if *Accumulator x* is equal to 10^{12} - 1, *Accumulator x* should not be updated.

Req C.89 Update counters and *CVR* for online request

For each value of x for which **all** of the following are true:

- *Counter x* is active for the transaction,
- **and** the value of *Counter x* is less than 'FF',
- **and** 'Allow Counting' (byte 1, bit b4) in the *Counter x Profile Control* has the value 1b,
- **and** 'Include Online Requests' (byte 2, bit b8) in the *Counter x Control* has the value 1b,
- **and** the *Transaction CVM* is (one of) the CVM(s) allowing counting,
- **and either** of the following is true:
  - 'Include Only If International' (byte 1, bit b4) in the *Counter x Control* has the value 0b,
  - **or** the transaction is an international transaction,
- **and either** of the following is true:
  - 'Include Only If Not Accumulated' (byte 1, bit b5) in the *Counter x Control* has the value 0b,
  - **or** the transaction cannot be accumulated according to Req C.88 in any *Accumulator x*, which is active for the transaction,

Counter x shall be incremented by 1 in the *Counters Data* template.

If the new value of *Counter x* is greater than the Counter x Lower (Upper) Limit, 'Lower (Upper) Offline Transaction Count Limit Exceeded' (byte 3, bit b8 (b7)) in the *Card Verification Results (CVR)* shall be set to 1b.

12.2.7 Respond to GENERATE AC Command

12.2.7.1 Build Issuer Application Data

Req 15.81 in Section 15.5.8.1 of [CPA] is replaced with the following requirements, Table and Notes.

Req C.90 Build *Issuer Application Data* for other profiles

If the *Profile ID* is **not** '7E', then the application shall build the *Issuer Application Data (IAD)* to be sent in the response, coded as specified in the CCD Part of [EMV 3], Annex C.7, for a CCD-compliant application with a Format Code of 'A', with:

- For each *Accumulator x* that is active for the transaction **and** for which 'Send Accumulator in IAD' in the *Accumulator Profile Control* for *Accumulator x* has the value 1b:
  - If 'Send Accumulator Balance' in the *Accumulator Profile Control* for *Accumulator x* has the value 1b, then the value (Accumulator x Upper Limit minus *Accumulator x*) shall be sent.
  - Otherwise ('Send Accumulator Balance' = 0b) the value of *Accumulator x* shall be sent.
- The profile-specific requirements shown in Table 9.
- If 'Encipher Counters Portion of IAD' in the *Issuer Options Profile Control* has the value 1b, then:
  - the Counters portion (bytes 9-16) of the *Issuer Application Data* shall be enciphered according to Req 20.14 in Section 20.5 of [CPA] as replaced by Specification Bulletin 165 before generating the Application Cryptogram,
  - the 8-byte enciphered Counters shall replace the 8-byte Counters portion before generating the *Application Cryptogram*.
- If **all** of the following are true:
  - 'Profile CCI' in the *Issuer Options Profile Control* has the value 'A6',
  - **and** 'Encipher Counters Portion of IAD' in the *Issuer Options Profile Control* has the value 1b,
  - and 'Mode of AES Encipherment' in the *Issuer Options Profile Control* has the value 1b (Encipher Counters and IDD),

  then
  - the IDD portion (bytes 19-32) of the *Issuer Application Data* shall be enciphered according to Req C.151 in Section 15.3,
  - the 14-byte enciphered IDD shall replace the 14-byte IDD portion before generating the *Application Cryptogram*.

Note:

Building the *Issuer Application Data* according to this specification takes into account, that additional data elements (*Accumulator 3*, *Counter 4*, Offline Transactions End Date, *Static Issuer Data*, *Dynamic Issuer Data*) may be included in the IDD.

If none of these additional data elements is to be included in the IDD, then building the *Issuer Application Data* according to this specification is the same as building the *Issuer Application Data* according to [CPA].

IAD Byte	Description	Value
1	Length	'0F'
2	CCI	Set to the value of the Profile CCI in the *Issuer Options Profile Control* for the transaction ('A5' or 'A6' for CCD-compliant profiles)
3	DKI	Set to the value of the Profile DKI in the *Issuer Options Profile Control* for the transaction
4-8	CVR	Set by application processing
9-16	Counters	See Req C.91
17	Length	'0F'
18	Profile ID	Set to the *Profile ID* used for the transaction
19-32	IDD	See Req C.92

Table 9: *Issuer Application Data* for Profile Not '7E'

Req C.91	**Build Counters in *Issuer Application Data* for other profiles**

Begins with the following:

- If *Accumulator 1* is active for the transaction **and** 'Send Accumulator in IAD' in the *Accumulator Profile Control* for *Accumulator 1* has the value 1b, then *Accumulator 1* (Value or Balance) is sent in Counters bytes 1-6.
- Otherwise, if *Accumulator 2* is active for the transaction **and** 'Send Accumulator in IAD' in the *Accumulator Profile Control* for *Accumulator 2* has the value 1b, then *Accumulator 2* (Value or Balance) is sent in Counters bytes 1-6.
- Otherwise, if *Accumulator 3* is active for the transaction **and** 'Send Accumulator in IAD' in the *Accumulator Profile Control* for *Accumulator 3* has the value 1b, then *Accumulator 3* (Value or Balance) is sent in Counters bytes 1-6.
- Otherwise, if VLP Available Funds is active for the transaction **and** 'Send Accumulator in IAD' in the *VLP Profile Control* has the value 1b, then the *VLP Available Funds* is sent in Counters bytes 1-6.

The remaining bytes shall contain the values of each *Counter x* that is active for the transaction **and** for which 'Send Counter in IAD' in the *Counter Profile Control* for *Counter x* has the value 1b, in priority order based upon the counter number (that is, the value of x for *Counter x*), with the lowest numbered counter having the highest priority.

The default value for these bytes is personalised in bytes 9-16 of the *Default Issuer Application Data*. Any portion of these bytes not filled with an accumulator or counter shall use the default value.

Req C.92 Build IDD in *Issuer Application Data* for other profiles

If more than one accumulator is to be sent in the IAD, these bytes contain the remaining accumulator(s) that were not sent in bytes 9-16, in the order shown:

- *Accumulator 2* (Value or Balance) if *Accumulator 2* is active for the transaction **and** 'Send Accumulator in IAD' in the *Accumulator Profile Control* for *Accumulator 2* has the value 1b.
- *Accumulator 3* (Value or Balance) if *Accumulator 3* is active for the transaction **and** 'Send Accumulator in IAD' in the *Accumulator Profile Control* for *Accumulator 3* has the value 1b.
- *VLP Available Funds* if VLP is supported **and** VLP Available Funds is active for the transaction **and** 'Send Accumulator in IAD' in the *VLP Profile Control* has the value 1b.

The remaining bytes shall contain the values of each *Counter x* not included in bytes 9-16 that is active for the transaction **and** for which 'Send Counter in IAD' in the *Counter Profile Control* for *Counter x* has the value 1b; in priority order based upon the counter number (that is, the value of x for *Counter x*), with the lowest numbered counter having the highest priority.

If at least 3 bytes remain in the IDD after including accumulator(s) and/or counter(s) as described above **and** if 'Include Offline Transactions End Date in IAD' in the *Issuer Options Profile Control* has the value 1b then the Offline Transactions End Date shall be included in the IDD according to Req C.93.

If at least 1 byte remains in the IDD after including accumulator(s) and/or counter(s) and/or Offline Transactions End Date as described above **and** if 'Include Static Issuer Data in IAD' in the *Issuer Options Profile Control* has the value 1b and if the *Static Issuer Data* are present in the application, then the *Static Issuer Data* or, if the *Static Issuer Data* consist of more bytes than remain in the IDD, the leftmost byte(s) of the *Static Issuer Data* shall be included in the IDD.

If at least 1 byte remains in the IDD after including accumulator(s) and/or counter(s) and/or Offline Transactions End Date and/or *Static Issuer Data* as described above **and** if 'Include Dynamic Issuer Data in IAD' in the *Issuer Options Profile Control* has the value 1b and if the *Dynamic Issuer Data* are present in the application, then the *Dynamic Issuer Data* or, if the *Dynamic Issuer Data* consist of more bytes than remain in the IDD, the leftmost byte(s) of the *Dynamic Issuer Data* shall be included in the IDD.

The default value for these bytes is personalised in bytes 19-32 of the *Default Issuer Application Data*. Any portion of these bytes not filled with an accumulator or counter shall use the default value.

Note:

If less than 3 bytes remain in the IDD after including accumulator(s) and/or counter(s) then the Offline Transactions End Date shall not be included in the IDD, but *Static Issuer Data* and/or *Dynamic Issuer Data* may still be included in the IDD.

Req C.93 Include Offline Transactions End Date

If the *Number of Days Offline Limit* or the *Last Online Transaction Date in Days* is missing in the application or is not formatted correctly, the 3-byte value '00 01 01' shall be included in the IDD as Offline Transactions End Date.

Otherwise,

Offline Transactions End Date in days

:= *Last Online Transaction Date* + *Number of Days Offline Limit*

shall be computed.

If the resulting value is greater than 36525, the 3-byte value '991231' shall be included in the Issuer Discretionary Data as Offline Transactions End Date.

If the resulting value is less than 36526, the Offline Transactions End Date in days shall be converted to a date in the format YYMMDD as described in Annex E of [CPA]. The resulting 3-byte value (in the format YYMMDD) shall be included in the IDD as Offline Transactions End Date.

12.2.7.2 Log Transaction

Section 15.5.8.3 of [CPA] is replaced with the following text. In particular, Req 15.82 in 15.5.8.3 of [CPA] is replaced with Req C.94.

If the issuer chooses to log transactions, then the application appends the information to the Transaction Log.

If the issuer chooses to log transactions and the response to the First GENERATE AC is an ARQC, but online requests shall not be logged for the first GENERATE AC command, then the application will need to save data to be logged during the Second GENERATE AC (see Section 17.4.1 of this specification).

Req C.94	**Log transaction at first GENERATE AC**

Prior to responding to the GENERATE AC command, if **all** of the following are true:

- the 'Log Transactions' bit in the *Issuer Options Profile Control* has the value 1b,
- **and** the Profile ID for the transaction does not have the value '7E',
- **and either** of the following is true:
  - **both** of the following are true:
    - the response is a TC type Application Cryptogram,
    - **and** 'Log Approved Transactions' in the *Application Control* has the value 1b,
  - **or both** of the following are true:
    - the response is an AAC type Application Cryptogram,
    - and 'Log Declined Transactions' in the *Application Control* has the value 1b,
  - **or both** of the following are true:
    - the response is an ARQC type Application Cryptogram,
    - and 'Log Online Requests' in the *Application Control* has the value 1b,

then the application shall append to the Transaction Log the value only (omitting the tag and length) for the data elements listed in Table 10, in the order shown

Data to Log	**Condition**
Amount, Authorised	always
Transaction Currency Code	always
Transaction Date	always
CVR	if 'Log the CVR' bit in *Application Control* = 1b
ATC	if 'Log the ATC' bit in *Application Control* = 1b
CID	if 'Log the CID' bit in *Application Control* = 1b
Profile ID	if 'Log the Profile ID' bit in *Application Control* = 1b

Data to Log	Condition
Data Extracted from the First GENERATE AC Command Data using the *First GENERATE AC Unchanging Log Data Table*	if any
Data Extracted from the First GENERATE AC Command Data using the *First GENERATE AC Log Data Table*	if any
Additional card data	if Internal Data Logging implementer-option is supported and *Internal Log Data Object List (ILDOL)* is present

Table 10: Transaction Log Entry for First GENERATE AC Logging

12.2.7.3 Store Transaction Data

Req C.95 Store transaction data for State SCRIPT

If the response to the first GENERATE AC command is a TC or an AAC, i.e. if the CPACE application transitions to the State SCRIPT, then the following data shall be stored transiently for Issuer-to-Card Script Processing:

- 'Script Received' flag and 'Script Failed' flag, initialised to 0.
- the 8-byte *Application Cryptogram (AC)*

Req C.96 Store transaction data for State ONLINE

If the response to the first GENERATE AC is an ARQC, i.e. if the CPACE application transitions to the State ONLINE, then the following data shall be stored transiently for Issuer-to-Card Script Processing and second GENERATE AC processing:

- 'Script Received' flag and 'Script Failed' flag, initialised to 0,
- the 8-byte *Application Cryptogram* (ARQC),
- *Application Decisional Results (ADR)*,
- *Card Verification Results (CVR)*,
- *Profile ID*,
- first GENERATE AC command data,
- GPO Input Data, already stored during the processing of the GET PROCESSING OPTIONS command for CDA computation,
- optionally, in order to avoid re-retrieval, the data elements listed in Table 11 retrieved from the first GENERATE AC command data.

Position	Data Element	Length (in bytes)	Format
Bytes 1 - 6	*Amount, Authorised*	6	n 12
Bytes 7 - 12	*Amount, Other*	6	n 12
Bytes 13 - 14	*Terminal Country Code*	2	n 3
Bytes 20 - 21	*Transaction Currency Code*	2	n 3
Bytes 22 - 24	*Transaction Date*	3	YYMMDD
Byte 25	*Transaction Type*	1	n 2
Bytes 31 - 33	*CVM Results*	3	b

Table 11: First GENERATE AC Command Data to be Stored Transiently

12.2.7.4 Return GENERATE AC Response

Section 15.5.8.4 of [CPA] is replaced with the following text.

Req C.97 Data field in first GENERATE AC response message

The data field in the first GENERATE AC response message returned by the CPACE application shall be coded

- as shown in Table 12, if no CDA signature is returned,
- as shown in Table 13, if a CDA signature is returned.

Tag	Value		Presence
'77'	*Response Message Template Format 2*		M
	'9F27'	*Cryptogram Information Data (CID)*	M
	'9F36'	*Application Transaction Counter (ATC)*	M
	'9F26'	*Application Cryptogram (AC)*	M
	'9F10'	*Issuer Application Data (IAD)*	M

Table 12: First GENERATE AC Response Message Data Field - No CDA

Tag	Value		Presence
'77'	*Response Message Template Format 2*		M
	'9F27'	*Cryptogram Information Data (CID)*	M
	'9F36'	*Application Transaction Counter (ATC)*	M
	'9F4B'	*Signed Dynamic Application Data (SDAD)*	M
	'9F10'	*Issuer Application Data (IAD)*	M

Table 13: First GENERATE AC Response Message Data Field - CDA

Req C.98 Generate CDA signature on TC, ARQC and AAC if requested

If **both** of the following are true:

- CDA processing is requested by the terminal (that is, 'CDA Requested' in the P1 parameter in the GENERATE AC command from the terminal was set to 1b),
- **and either** of the following is true:
  - the CPACE application is responding with either an ARQC or TC type *Application Cryptogram*,
  - **or all** of the following are true:
    - the CPACE application is responding with an AAC type *Application Cryptogram*,
    - **and** an offline decline has been requested by the terminal,
    - **and** 'Interface' in *Environment in Use* = CONTACTLESS,

then the CPACE application

- shall generate a dynamic signature as described in Req C.99, including the tags, lengths, and values of the data elements returned in the *Response Message Template Format 2* shown in Table 13 in the order they are returned, with the exception of the *Signed Dynamic Application Data*,
- shall return a first GENERATE AC response with a response message data field shown in Table 13.

Otherwise, the CPACE application shall return a first GENERATE AC response with a response message data field shown in Table 12.

Req C.99 Generate dynamic signature

If the Relay Resistance Protocol implementer-option is not supported or if *RRP Counter* = 0, then the dynamic signature shall be generated as described in Section 6.6.1 of [EMV 2].

If the Relay Resistance Protocol implementer-option is supported and if *RRP Counter* > 0, then the dynamic signature shall be generated as described in Section 6.6.1 of [EMV 2] with the following modification:

The Dynamic Application Data to be Signed according to Table 18 in Section 6.6.1 of [EMV 2] shall be built as shown in Table 14.

This means that the ICC Dynamic Data to be included in the Dynamic Application Data to be Signed

- are built as concatenation of the "Standard ICC Dynamic Data", i.e. the data elements listed in Table 19 in Section 6.6.1 of [EMV 2] with an 8-byte *ICC Dynamic Number* and the *RRP Transaction Data Set* stored transiently during EXCHANGE RELAY RESISTANCE DATA Command Processing (see Section 8.2.3):

  ICC Dynamic Data = Standard ICC Dynamic Data | *RRP Transaction Data Set*

- and have a length L_{DD} of 52 bytes.

Field Name	Length (in bytes)	Value	Format
Signed Data Format	1	'05'	b
Hash Algorithm Indicator	1	'01'	b
ICC Dynamic Data Length L_{DD}	1	'34'	b
ICC Dynamic Data	1	'08'	b
	8	*ICC Dynamic Number*	b
	1	*Cryptogram Information Data*	b
	8	*Application Cryptogram*	b
	20	Transaction Data Hash Code	b
	14	*RRP Transaction Data Set*	b
Pad Pattern	N_{IC} - 77	Padding bytes 'BB'	b
Unpredictable Number	4	*Unpredictable Number*	b

Table 14: Dynamic Application Data to be Signed Including RRP Data

13 Second Card Action Analysis

13.1 Introduction

This section refers to Section 17 of [CPA]:

- A modification regarding Section 17.5.1 of [CPA] (Command Coding) is described in Section 13.2.1.
- Part of Section 17.5.2 of [CPA] has been modified and moved to Section 13.2.2 (Configure Second Card Analysis - First Part).
- Modifications regarding Section 17.5.1.1 of [CPA] (Command Format Validation) are described in Section 13.2.3.
- A modification regarding Issuer Authentication Processing in Section 17.5.3.1 of [CPA] is described in Section 13.2.4.
- Additional requirements regarding Section 17.5.3.1.2 of [CPA] (Issuer Authentication Passed) are described in Section 13.2.5.
- Modifications and additional requirements regarding Section 17.5.3.1.3 of [CPA] (CSU and *PAD* Processing) are described in Section 13.2.6.
- Modifications and additional requirements regarding Sections 17.5.4.1.1, 17.5.4.1.2, 17.5.4.1.4 and 17.5.4.1.5 of [CPA] (Accumulator x and Counter x Velocity Checking) are described in Section 13.2.7.1.
- An additional Card Risk Management check (Cashback Check) defined by this specification is described in Section 13.2.7.2.
- Modifications regarding Section 17.5.4.2.2 of [CPA] (Application Approves Transaction Offline (Unable to Go Online)) are described in Section 13.2.8.
- Additional requirements regarding Section 17.5.8.1 of [CPA] (Build Issuer Application Data) are described in Section 13.2.9.1.
- A modification regarding Section 17.5.8.3 of [CPA] (Log Transactions) is described in Section 13.2.9.2.
- Modifications and additional requirements regarding Section 17.5.8.4 of [CPA] (Return GENERATE AC Response) are described in Section 13.2.9.3.

13.2 Second GENERATE AC Command

13.2.1 Command Coding

Req 17.2 in Section 17.5.1 of [CPA] is replaced with the following text.

Req C.100 Interpretation of second GENERATE AC command data

Interpretation of contents and length of the second GENERATE AC command data field depends on the values of 'Amounts Included in CDOL2' in the *Application Control* and 'Proprietary Authentication Data in IATD Supported' in the *Issuer Options Profile Control*.

If 'Amounts Included in CDOL2' in the *Application Control* has the value 1b, and if 'Proprietary Authentication Data in IATD Supported' in the *Issuer Options Profile Control* has the value 0b, then the second GENERATE AC command data field shall be interpreted as consisting of the data elements listed in Table 17-5 in Section 17.5.1 of [CPA], in the order shown.

If 'Amounts Included in CDOL2' in the *Application Control* has the value 0b, and if 'Proprietary Authentication Data in IATD Supported' in the *Issuer Options Profile Control* has the value 0b, then the second GENERATE AC command data field shall be interpreted as consisting of the data elements listed in Table 17-6 in Section 17.5.1 of [CPA], in the order shown.

If 'Amounts Included in CDOL2' in the *Application Control* has the value 1b, and if 'Proprietary Authentication Data in IATD Supported' in the *Issuer Options Profile Control* has the value 1b, then the second GENERATE AC command data field shall be interpreted as consisting of the data elements listed in Table 15, in the order shown.

If 'Amounts Included in CDOL2' in the *Application Control* has the value 0b, and if 'Proprietary Authentication Data in IATD Supported' in the *Issuer Options Profile Control* has the value 1b, then the second GENERATE AC command data field shall be interpreted as consisting of the data elements listed in Table 16, in the order shown.

Position	Data Element	Length (in bytes)	Format
Bytes 1 - 16	*Issuer Authentication Data (IATD)*, possibly padded	16	b
Bytes 17 - 18	*Authorisation Response Code (ARC)*	2	an 2
Bytes 19 - 23	*Terminal Verification Results (TVR)*	5	b
Bytes 24 - 27	*Unpredictable Number*	4	b
Bytes 28 - 33	*Amount, Authorised*	6	n 12
Bytes 34 - 39	*Amount, Other*	6	n 12
Bytes 40 - (39+L)	Second GENERATE AC Extension Data of length L	var.	b

Table 15: Second GENERATE AC Command Data Field: Amounts and Proprietary Authentication Data in CDOL2

Position	Data Element	Length (in bytes)	Format
Bytes 1 - 16	*Issuer Authentication Data (IATD)*, possibly padded	16	b
Bytes 17 - 18	*Authorisation Response Code (ARC)*	2	an 2
Bytes 19 - 23	*Terminal Verification Results (TVR)*	5	b
Bytes 24 - 27	*Unpredictable Number*	4	b
Bytes 28 - (27+L)	Second GENERATE AC Extension Data of length L	var.	b

Table 16: Second GENERATE AC Command Data Field: Proprietary Authentication Data and No Amounts in CDOL2

13.2.2 Configure Second Card Analysis - First Part

The first and second paragraph, the paragraph preceding Req 17.12 and Req 17.12 in Section 17.5.2 are replaced with the following text.

The CPACE application only performs Second Card Action Analysis processing when the application requested an online authorisation during First Card Action Analysis.

The data elements that were stored transiently in volatile memory during first GENERATE AC processing (see Section 12.2.7.3) are still available for further transaction processing.

In particular, the *Profile ID* to be used for the transaction has been stored during the processing of the first GENERATE AC. It identifies the *Profile Control* to be used to configure the application behaviour for Card Action Analysis.

Req C.101	**Update Profile Configuration**
If data elements retrieved from non-volatile memory during first GENERATE AC processing have been changed during Issuer-to-Card Script Processing, the values of these data elements shall be (re-)retrieved from non-volatile memory, when they are used the first time during the processing of the second GENERATE AC command. For the retrieval of the *Profile Control*, *Issuer Options Profile Control*, *Accumulator x Control* and *Accumulator Profile Control y, Counter x Control* and *Counter Profile Control y* Req C.46, Req C.47, Req C.78, Req C.79 apply.	

13.2.3 Command Format Validation

Req 17.7 and Req 17.8 in Section 17.5.1.1 of [CPA] are replaced with the following requirement.

Req C.102	**Check value of Lc using *Application Control* and *Issuer Options Profile Control***

If **either** of the following is true:

- 'Proprietary Authentication Data in IATD Supported' in the *Issuer Options Profile Control* has the value 0b,
- **and either** of the following is true:
  - 'Amounts Included in CDOL2' in the *Application Control* has the value 0b and the value of Lc is less than 19,
  - **or** 'Amounts Included in CDOL2' in the *Application Control* has the value 1b and the value of Lc is less than 31,
- **or** 'Proprietary Authentication Data in IATD Supported' in the *Issuer Options Profile Control* has the value 1b,
- **and either** of the following is true:
  - 'Amounts Included in CDOL2' in the *Application Control* has the value 0b and the value of Lc is less than 27,
  - **or** 'Amounts Included in CDOL2' in the *Application Control* has the value 1b and the value of Lc is less than 39,

then the CPACE application shall discontinue processing the command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6700' (Wrong Length).

The following requirement is added at the end of Section 17.5.1.1 of [CPA].

Req C.103	**Validation of the second GENERATE AC command data field**

If **both** of the following are true:

- 'Proprietary Authentication Data in IATD Supported' in the *Issuer Options Profile Control* has the value 0b,
- **and** 'Proprietary Authentication Data (PAD) Included' in the *Card Status Update (CSU)*, that is bit b8 of byte 5 of the second GENERATE AC command data field, has the value 1b,

then the CPACE application shall discontinue processing the command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6985' (Conditions of use not satisfied).

The length L_P of the *Proprietary Authentication Data (PAD)* shall be determined in the following way:

- If **either** of the following is true:
  - 'Proprietary Authentication Data (PAD) Included' in the *Card Status Update (CSU)* has the value 0b,
  - **or** all of the bits b8-b5 of byte 4 of the *Card Status Update (CSU)*, that is bits b8-b5 of byte 8 of the second GENERATE AC command data field, have the value 0b,

  then *Proprietary Authentication Data (PAD)* are not present in the *Issuer Authentication Data (IATD)*, that is, $L_P = 0$.
- Otherwise, that is if **both** of the following are true:
  - 'Proprietary Authentication Data (PAD) Included' in the *Card Status Update (CSU)* has the value 1b,
  - **and** at least one of the bits b8-b5 of byte 4 of the *Card Status Update (CSU)* has the value 1b,

  then 8-byte *Proprietary Authentication Data (PAD)* are present in the *Issuer Authentication Data (IATD)*, that is, $L_P = 8$.

If command format validation is passed successfully, the command data field of the second GENERATE AC command (called **second GENERATE AC command data**) shall be retrieved for further processing.

13.2.4 Issuer Authentication Processing

The note in the description of step 2 in Section 17.5.3.1 of [CPA] is replaced with the following requirement.

Req C.104 Generation of the ARPC

The Application Cryptogram Session Key SK_{AC} which has been derived during first GENERATE AC processing shall be used to generate the ARPC.

According to this specification, *Proprietary Authentication Data (PAD)* are supported and shall be used in the generation of the ARPC according to the description in Section 8.2.2 of [EMV 2]. The length L_P of the *Proprietary Authentication Data (PAD)* to be included in ARPC generation has been determined according to Req C.103.

Note:

According to Req C.103, even if 'Proprietary Authentication Data (PAD) Included' in the *Card Status Update (CSU)* has the value 1b, the length L_P of the *Proprietary Authentication Data (PAD)* to be included in ARPC generation may be 0.

13.2.5 Issuer Authentication Passed

The following requirements are inserted between Req 17.37 and Req 17.38 in Section 17.5.3.1.2 of [CPA].

Req C.105	**Activate contactless access to card - Issuer Authentication**

If **all** of the following are true:

- The Contactless Control - Card implementer-option is supported,
- **and** the interface currently used is contact,
- **and** 'Right of application to activate/deactivate contactless access to the card' in *Contactless Control - Application* = ENABLED,
- **and** 'Activation of contactless access to the application with second GENERATE AC and successful Issuer Authentication on the contact interface' in *Contactless Control - Card* = ENABLED,

then contactless access to the CPACE card shall be activated and the (re-)deactivation mechanism for the card described in Req C.18 shall be disabled as follows:

- 'State of contactless access to the Card' in *Contactless Control - Card* shall be set to ACTIVATED,
- 'Enablement of unsecured DEACTIVATE CL command for the card' in *Contactless Control - Card* shall be set to DISABLED.

Note:

If *Contactless Control - Application* is not present in the CPACE application or if *Contactless Control - Card* is not present in the CPACE card, then the CPACE application shall use the value '80' (see Section 16.7). In this case contactless access to the CPACE card will remain unchanged.

Req C.106	**Activate contactless access to application - Issuer Authentication**

If **all** of the following are true:

- The Contactless Control - Application implementer-option is supported,
- **and** the interface currently used is contact,
- **and** 'Activation of contactless access to the application with second GENERATE AC and successful Issuer Authentication on the contact interface' in *Contactless Control - Application* = ENABLED,

then contactless access to the CPACE application shall be activated and the (re-)deactivation mechanism for the application described in Req C.12 shall be disabled as follows:

- 'State of contactless access to the application' in *Contactless Control - Application* shall be set to ACTIVATED,
- 'Enablement of unsecured DEACTIVATE CL command for the application' in *Contactless Control - Application* shall be set to DISABLED.

Note:

If *Contactless Control - Application* is not present in the CPACE application, then the CPACE application shall use the value '80' (see Section 16.7). In this case contactless access to the CPACE application will remain unchanged.

13.2.6 CSU and *PAD* Processing

According to this specification, *Proprietary Authentication Data (PAD)* may be returned by the issuer in the *Issuer Authentication Data (IATD)* in order to perform one or more of the following steps:

- Update the *Number of Days Offline Limit*,
- Update Accumulator 1 Upper Limit 0 or Accumulator 1 Upper Limit 1,
- Update accumulators and counters individually.

In addition, according to this specification, the *Card Status Update (CSU)* may be used by the issuer to activate or deactivate contactless access to the CPACE dual interface card when the Contactless Control - Card implementer-option is supported or to activate or deactivate contactless access to the CPACE application on a dual interface card when the Contactless Control - Application implementer-option is supported.

The first paragraph in Section 17.5.3.1.3 of [CPA] is replaced with the following text and requirement.

After successful Issuer Authentication, the CPACE application has verified that the *Card Status Update (CSU)* received in Issuer Authentication Data is valid.

Req C.107	**CSU Coding**
The *Card Status Update (CSU)* for the CPACE application interpreted shall be coded according to Section 21.23 of this specification. With the exception of byte 3, this coding conforms to the Common Core Definitions part of [EMV 3], for a Cryptogram Version of '5' or '6'. Byte 3 in the *Card Status Update (CSU)* shall only be interpreted as being coded according to Section 21.23 of this specification, if the Contactless Control - Card implementer-option is supported or if the Contactless Control - Application implementer-option is supported. If neither the Contactless Control - Card implementer-option nor the Contactless Control - Application implementer-option is supported, then byte 3 in the *Card Status Update (CSU)* shall not be evaluated.	

The following requirements are inserted in Section 17.5.3.1.3 of [CPA] after Req 17.39 and its explanation, i.e. after the paragraph reading as follows:

> This blocks the application; which causes the card to respond to all subsequent SELECT commands with status bytes indicating that the selected file is invalidated, and to respond to all subsequent GENERATE AC commands with an AAC type Application Cryptogram.

Req C.108 Activate contactless access to card with CSU

If **all** of the following are true:

- the Contactless Control - Card implementer-option is supported,
- **and** 'Right of application to activate/deactivate contactless access to the card' in *Contactless Control - Application* = ENABLED,
- **and** 'Activate contactless' in *Card Status Update (CSU)* = ACTIVATE,
- **and** 'Apply activation/deactivation of contactless to' in *Card Status Update (CSU)* = CARD,
- **and** *Contactless Control - Card* is present in the CPACE card,

then the following steps shall be performed:

- 'State of contactless access to the card' in *Contactless Control - Card* shall be set to ACTIVATED,
- 'Enablement of unsecured DEACTIVATE CL command for the card' in *Contactless Control - Card* shall be set to DISABLED.

Note:

If *Contactless Control - Application* is not present in the CPACE application, then the CPACE application shall use the value '80' (see Section 16.7). In this case contactless access to the CPACE card will remain unchanged.

Req C.109 Deactivate contactless access to card with CSU

If **all** of the following are true:

- the Contactless Control - Card implementer-option is supported,
- **and** 'Right of application to activate/deactivate contactless access to the card' in *Contactless Control - Application* = ENABLED,
- **and** 'Deactivate contactless' in *Card Status Update (CSU)* = DEACTIVATE,
- **and** 'Apply activation/deactivation of contactless to' in *Card Status Update (CSU)* = CARD,
- **and** *Contactless Control - Card* is present in the CPACE card,

then the following steps shall be performed:

- 'State of contactless access to the card' in *Contactless Control - Card* shall be set to DEACTIVATED,
- 'Activation of contactless access to the card with SELECT of an application on the contact interface' in *Contactless Control - Card* shall be set to DISABLED,
- 'Activation of contactless access to the card with successful VERIFY command on the contact interface' in *Contactless Control - Card* shall be set to DISABLED,
- 'Activation of contactless access to the card with second GENERATE AC and successful Issuer Authentication on the contact interface' in *Contactless Control - Card* shall be set to DISABLED.

Note:

If *Contactless Control - Application* is not present in the CPACE application, then the CPACE application shall use the value '80' (see Section 16.7). In this case contactless access to the CPACE card will remain unchanged.

Req C.110	**Activate contactless access to application with CSU**

If **all** of the following are true:

- the Contactless Control - Application implementer-option is supported,
- **and** 'Activate contactless' in *Card Status Update (CSU)* = ACTIVATE,
- **and** 'Apply activation/deactivation of contactless to' in *Card Status Update (CSU)* = APPLICATION,
- **and** *Contactless Control - Application* is present in the CPACE application,

then the following steps shall be performed:

- 'State of contactless access to the application' in *Contactless Control - Application* shall be set to ACTIVATED,
- 'Enablement of unsecured DEACTIVATE CL command for the application' in *Contactless Control - Application* shall be set to DISABLED.

Req C.111	**Deactivate contactless access to application with CSU**

If **all** of the following are true:

- the Contactless Control - Application implementer-option is supported,
- **and** 'Deactivate contactless' in *Card Status Update (CSU)* = DEACTIVATE,
- **and** 'Apply activation/deactivation of contactless to' in *Card Status Update (CSU)* = APPLICATION,
- **and** *Contactless Control - Application* is present in the CPACE application,

then the following steps shall be performed:

- 'State of contactless access to the application' in *Contactless Control - Application* shall be set to DEACTIVATED,
- 'Activation of contactless access to the application with SELECT of the application on the contact interface' in *Contactless Control - Application* shall be set to DISABLED,
- 'Activation of contactless access to the application with successful VERIFY command on the contact interface' in *Contactless Control - Application* shall be set to DISABLED,
- 'Activation of contactless access to the application with second GENERATE AC and successful Issuer Authentication on the contact interface' in *Contactless Control - Application* shall be set to DISABLED.

Requirements Req 17.41 to Req 17.46 in Section 17.5.3.1.3 of [CPA] are replaced with the following requirements.

Req C.112 Update of limits

The update of limits shall only be performed, if **all** of the following are true:

- 'Proprietary Authentication Data in IATD Supported' in the *Issuer Options Profile Control* has the value 1b,
- **and** 'Proprietary Authentication Data (PAD) Included' in the *CSU* has the value 1b,
- **and either** of the following is true:
  - 'New Number of Days Offline Limit' (byte 4, bit b7) in the *CSU* has the value 1b,
  - **or** 'New Accumulator 1 Upper Limit's (byte 4, bit b6-b5) in the *CSU* have a value that is different from 00b.

In this case the update of limits shall be processed as described below using the *PAD* (see Table 76) retrieved from bytes 9 to 16 of the second GENERATE AC command data.

- If and only if **both** of the following are true:
  - 'New Number of Days Offline Limit' (byte 4, bit b7) in the *CSU* has the value 1b,
  - **and** bytes 2 and 3 of the *PAD* have the format n 4,

  the *Number of Days Offline Limit* shall be updated with bytes 2 and 3 of the *PAD*.
- If and only if **both** of the following are true:
  - 'Limit 0' (byte 4, bit b6) in the *CSU* has the value 1b,
  - **and** bytes 4 to 8 of the *PAD* have the format n 10,

  Accumulator 1 Upper Limit 0 shall be updated in the following way:
  - Byte 1 of the Accumulator 1 Upper Limit 0 shall be set to '00'.
  - Bytes 2 to 6 of the Accumulator 1 Upper Limit 0 shall be updated with bytes 4 to 8 of the *PAD*.
- If and only if **both** of the following are true:
  - 'Limit 1' (byte 4, bit b5) in the *CSU* has the value 1b,
  - **and** bytes 4 to 8 of the *PAD* have the format n 10,

  Accumulator 1 Upper Limit 1 shall be updated in the following way:
  - Byte 1 of the Accumulator 1 Upper Limit 1 shall be set to '00'.
  - Bytes 2 to 6 of the Accumulator 1 Upper Limit 1 shall be updated with bytes 4 to 8 of the *PAD*.

Note:

For the update of limits as described above it shall not be checked whether the

Maximum Number of Days Offline Check or Accumulator 1 is active for the transaction.

Req C.113 Assign Update Bits to Accumulators and Counters

If **either** of the following is true:

- 'CSU Created by Proxy for the Issuer' (byte 2, bit b3) in the *CSU* has the value 0b (the *CSU* was not created by a Proxy),
- **or** 'Use Default Update Counters to Control Offline Counters if *CSU* is generated by Issuer Proxy' (byte 2, bit b8) in the *Application Control* has the value 0b (use the *CSU* bits even if the *CSU* was created by a Proxy),

then accumulators and counters shall be set according to Req C.114, Req C.115, Req C.116, Req C.117 and Req C.118 using the Update Bits, which shall be assigned to each accumulator and counter in the following way:

- If **all** of the following are true:
  - 'Proprietary Authentication Data in IATD Supported' (byte 7, bit b4) in the *Issuer Options Profile Control* has the value 1b,
  - **and** 'Proprietary Authentication Data (PAD) Included' (byte 1, bit b8) in the *CSU* has the value 1b,
  - **and** 'Individual Update of Accumulators and Counters' (byte 4, bit b8) in the *CSU* has the value 1b,

  individual Update Bits shall be assigned to each accumulator and counter as shown in Table 17.
- Otherwise, that is if **any** of the following is true:
  - 'Proprietary Authentication Data in IATD Supported' (byte 7, bit b4) in the *Issuer Options Profile Control* has the value 0b,
  - **or** 'Proprietary Authentication Data (PAD) Included' (byte 1, bit b8) in the *CSU* has the value 0b,
  - **or** 'Individual Update of Accumulators and Counters' (byte 4, bit b8) in the *CSU* has the value 0b,

  'Update Counters' (byte 2, bits b2-b1) in the *CSU* shall be assigned to all accumulators and counters as Update Bits.

Otherwise, that is if **both** of the following are true:

- 'CSU Created by Proxy for the Issuer' (byte 2, bit b3) in the *CSU* has the value 1b (the *CSU* was created by a Proxy),
- **and** 'Use Default Update Counters to Control Offline Counters if CSU is generated by Issuer Proxy' (byte 2, bit b8) in the *Application Control* has the value 1b (use 'Default Update Counters' in the *Application Control* if the *CSU* was created by a Proxy),

then accumulators and counters shall be set according to Req C.114, Req C.115, Req C.116, Req C.117 and Req C.118 using 'Default Update Counters' (byte 2, bits b7-b6) in the *Application Control* as Update Bits assigned to all accumulators and counters.

Update Bits	**Assigned to**
'Update Accumulator 1' (byte 2, bits b2-b1) in the *CSU*	Accumulator 1
'Update Accumulator 2' (byte 4, bits b4-b3) in the *CSU*	Accumulator 2
'Update Accumulator 3' (byte 4, bits b2-b1) in the *CSU*	Accumulator 3
'Update Counter 1' (byte 1, bits b8-b7) in the *PAD*	Counter 1
'Update Counter 2' (Byte 1, bits b6-b5) in the *PAD*	Counter 2
'Update Counter 3' (byte 1, bits b4-b3) in the *PAD*	Counter 3
'Update Counter 4' (byte 1, bits b2-b1) in the *PAD*	Counter 4

Table 17: Individual Update Bits Assigned to Accumulators and Counters

Req C.114 Setting of accumulators and counters

The setting of accumulators and counters shall be performed as described below, using the Update Bits, which have been assigned to the accumulators and counters according to Req C.113.

- All Accumulators x and Counters x to which the Update Bits with the value 00b (Do Not Update Offline Accumulator/Counter) have been assigned shall remain unchanged.
- All Accumulators x and Counters x to which the Update Bits with the value 10b have been assigned shall be reset to 0 as described in Req C.115.
- All Accumulators x and Counters x to which the Update Bits with the value 01b have been assigned shall be set to their upper limit as described in Req C.116.
- The (Transaction Amount of the) online transaction shall be added to all Accumulators x and Counters x to which the Update Bits with the value 11b have been assigned as described in Req C.117 and Req C.118.

Req C.115	**Reset accumulators and counters to zero**

For each value of x for which **both** of the following are true:

- *Accumulator x* is active for the transaction,
- **and** 'Reset Accumulator with Online Response' (byte 1, bit b7) in the *Accumulator x Profile Control* has the value 1b,

Accumulator x shall be updated with the value 0.

For each value of x for which **both** of the following are true:

- *Counter x* is active for the transaction,
- **and** 'Reset Counter with Online Response' (byte 1, bit b3) in the *Counter x Profile Control* has the value 1b,

Counter x shall be updated with the value 0.

Req C.116	**Set accumulators and counters to their upper limit**

For each value of x for which **both** of the following are true:

- *Accumulator x* is active for the transaction,
- **and** 'Reset Accumulator with Online Response' (byte 1, bit b7) in the *Accumulator x Profile Control* has the value 1b,

Accumulator x shall be updated with the value of Accumulator x Upper Limit.

Note:

If *Accumulator 1* is set to its upper limit and Accumulator 1 Upper Limit has been updated according to Req C.112, the new value of Accumulator 1 Upper Limit shall be used to update *Accumulator 1*.

For each value of x for which **both** of the following are true:

- *Counter x* is active for the transaction,

  and 'Reset Counter with Online Response' (byte 1, bit b3) in the *Counter x Profile Control* has the value 1b,

Counter x shall be updated with the value of Counter x Upper Limit.

Req C.117 Add transaction to accumulators

This update shall be performed if and only if 'Issuer Approves Online Transaction' (byte 2, bit b8) in the *CSU* has the value 1b (issuer approves online transaction).

For each value of x for which **all** of the following are true:

- *Accumulator x* is active for the transaction,
- 'Allow Accumulation' (byte 1, bit b8) in the *Accumulator x Profile Control* has the value 1b,
- **and** the *Transaction CVM* is (one of) the CVM(s) allowing accumulation,
- **and either** of the following is true:
  - the transaction currency matches the accumulator currency,
  - **or** the transaction currency can be converted to the accumulator currency.

Accumulator x shall be updated as described below:

- If the transaction currency matches the accumulator currency:
  - If *Accumulator x* + Transaction Amount is (would be) greater than 10^{12} - 1,

    Accumulator x shall be updated with the value 10^{12} - 1.
  - Otherwise,

    Accumulator x shall be updated with

    Accumulator x + Transaction Amount.
- If the transaction currency does not match the accumulator currency (in which case the transaction currency can be converted to the accumulator currency), the Transaction Amount shall be converted to the Converted Transaction Amount in accumulator currency.
  - If the Converted Transaction Amount or *Accumulator x* + Converted Transaction Amount is (would be) greater than 10^{12} - 1,

    Accumulator x shall be updated with the value 10^{12} - 1.
  - Otherwise,

    Accumulator x shall be updated with

    Accumulator x + Converted Transaction Amount.

Note:

- If the (Converted) Transaction Amount is equal to 0 or if *Accumulator x* is equal to 10^{12} - 1, *Accumulator x* should not be updated.
- The Transaction CVM check, i.e. the check whether the *Transaction CVM* is (one of) the CVM(s) allowing accumulation shall be performed according to Req C.80 and Req C.81.

Req C.118 Add transaction to counters

For each value of x for which **all** of the following are true:

- *Counter x* is active for the transaction,
- **and** the value of *Counter x* is less than 'FF',
- **and** 'Allow Counting' (byte 1, bit b4) in the *Counter x Profile Control* has the value 1b,
- **and** the *Transaction CVM* is (one of) the CVM(s) allowing counting,
- **and either** of the following is true:
  - 'Include Only If International' (byte 1, bit b4) in the *Counter x Control* has the value 0b,
  - **or** the transaction is an international transaction,
- **and either** of the following is true:
  - 'Include Only If Not Accumulated' (byte 1, bit b5) in the *Counter x Control* has the value 0b,
  - **or** the transaction cannot be accumulated in any *Accumulator x*, which is active for the transaction,

Counter x shall be incremented by 1.

Note:

- The Transaction CVM check, i.e. the check whether the *Transaction CVM* is (one of) the CVM(s) allowing accumulation shall be performed according to Req C.80 and Req C.81.
- If and only if 'Include Only If Not Accumulated' (byte 1, bit b5) in the *Counter x Control* has the value 1b, it has to be checked, whether the transaction cannot be accumulated in any *Accumulator x*, which is active for the transaction.

  The transaction cannot be accumulated in any *Accumulator x*, which is active for the transaction, if 'Issuer Approves Online Transaction' (byte 2, bit b8) in the *CSU* has the value 0b (issuer declines online transaction) or if **any** of the following is true for all *Accumulators x*, which are active for the transaction:

  - the Update Bits assigned to *Accumulator x* do not have the value 11b (Add Transaction to Accumulator),
  - **or** 'Allow Accumulation' (byte 1, bit b8) in the *Accumulator x Profile Control* has the value 0b,
  - **or** the *Transaction CVM* is not (one of) the CVM(s) allowing accumulation,
  - **or both** of the following are true:
    - the transaction currency does not match the accumulator currency,
    - **and** the transaction currency cannot be converted to the accumulator currency.

  This has already been checked according to Req C.114 and Req C.117 and shall not be checked again now.

13.2.7 Second Card Risk Management

13.2.7.1 Accumulator x and Counter x Velocity Checking

According to this specification, the functionality of Velocity Checking for *Accumulator x* and *Counter x* described in [CPA] has been extended to support accumulation and counting based on the *Transaction CVM*. The Transaction CVM check, i.e. the check whether the *Transaction CVM* is (one of) the CVM(s) allowing accumulation or counting shall be performed as described in Req C.80 and Req C.81.

The following condition is inserted between the first and second of both ANDed sets of conditions of Req 17.60 and of Req 17.61 and between the second and third row of Table 17-12 in Section 17.5.4.1 of [CPA].

- the 'Allow Accumulation' bit in the *Accumulator Profile Control* for *Accumulator x* in this profile has the value 1b
- **and** the *Transaction CVM* is (one of) the CVM(s) allowing accumulation,
- **and** the 'Include Offline Approvals' bit in the *Accumulator x Control* has the value 1b,

The following condition is inserted between the first and second of the set ANDed set of conditions of Req 17.62 and of Req 17.63 in Section 17.5.4.1 of [CPA].

- the 'Allow Counting' bit in the *Counter Profile Control* for *Counter x* in this profile has the value 1b
- **and** the *Transaction CVM* is (one of) the CVM(s) allowing counting,
- **and** the 'Include Offline Approvals' bit in the *Counter x Control* has the value 1b,

13.2.7.2 Cashback Check

This issuer-optional check is defined by this specification. It identifies whether the current transaction is a transaction with cashback. This information is considered, when deciding whether to approve or decline the transaction offline, or to send the transaction online.

Req C.119 Cashback Check
The Cashback Check shall be performed if and only if **all** of the following are true: • 'Activate Cashback Check' (byte 7, bit b2) in the *Issuer Options Profile Control* has the value 1b, • **and** a TC was requested in the second GENERATE AC command, • **and** the CPACE application is not blocked. The Cashback Check shall be performed as described in Req C.83 using the current values of the parameters.

13.2.8 Application Approves Transaction Offline (Unable to Go Online)

According to this specification, the functionality of Velocity Checking for *Accumulator x* and *Counter x* described in [CPA] has been extended to support accumulation and counting based on the *Transaction CVM*. The Transaction CVM check, i.e. the check whether the *Transaction CVM* is (one of) the CVM(s) allowing accumulation or counting shall be performed as described in Req C.80 and Req C.81.

The following condition is inserted between the second and third condition of Req 17.72 in Section 17.5.4.2.2 of [CPA].

- the 'Allow Accumulation' bit in the *Accumulator Profile Control* for *Accumulator x* in this profile has the value 1b
- **and** the *Transaction CVM* is (one of) the CVM(s) allowing accumulation,
- **and** the 'Include Offline Approvals' bit in the *Accumulator x Control* has the value 1b,

The following condition is inserted between the first and second condition of Req 17.73 in Section 17.5.4.2.2 of [CPA].

- Counter x is active
- **and** the *Transaction CVM* is (one of) the CVM(s) allowing counting,
- **and** the 'Allow Counting' bit in the *Counter Profile Control* for *Counter x* in this profile has the value 1b

13.2.9 Respond to GENERATE AC Command

13.2.9.1 Build Issuer Application Data

Req 15.87 in Section 17.5.8.1 of [CPA] is replaced with the following requirement.

Req C.120	**Build IAD**
The *Issuer Application Data* shall be built as described in Req C.90, Req C.91, Req C.92, Req C.93, using the current values of the data elements that are included in the *Issuer Application Data*.	

13.2.9.2 Log Transactions

Req 17.88 in Section 17.5.8.3 of [CPA] is replaced with the following requirement.

Req C.121 Update Transaction Log

Prior to responding to the GENERATE AC command, if **both** of the following are true:

- the 'Log Transactions' bit in the *Issuer Options Profile Control* has the value 1b,
- **and any** of the following is true:
  - **all** of the following are true (all approvals are logged):
    - the response is a TC type Application Cryptogram
    - **and** the 'Log Approved Transactions' bit in the *Application Control* has the value 1b,
    - **and** the 'Log Offline Only' bit in the *Application Control* has the value 0b (log all approved transactions),
  - **or all** of the following are true (online approvals are not logged):
    - the response is a TC type Application Cryptogram
    - **and** the 'Log Approved Transactions' bit in the *Application Control* has the value 1b,
    - **and** the 'Log Offline Only' bit in the *Application Control* has the value 1b,
    - **and** the terminal was unable to go online (that is, the *ARC* was Y3),
  - **or both** of the following are true:
    - the response is an AAC type Application Cryptogram
    - **and** the 'Log Declined Transactions' bit in the *Application Control* has the value 1b

then the application shall

- append to the Transaction Log the value only (omitting the tag and length) for the data elements listed in Table 18, in the order shown, if 'Log Online Requests' in *Application Control* has the value 0b,
- replace the most recent record of the Transaction Log with the value only (omitting the tag and length) for the data elements listed in Table 18, in the order shown, if 'Log Online Requests' in *Application Control* has the value 1b.

Data to Log	Condition
Amount, Authorised	always
Transaction Currency Code	always
Transaction Date	always
CVR	if 'Log the CVR' bit in *Application Control* = 1b

Data to Log	Condition
ATC	if 'Log the ATC' bit in *Application Control* = 1b
CID	if 'Log the CID' bit in *Application Control* = 1b
Profile ID	if 'Log the Profile ID' bit in *Application Control* = 1b
Data Extracted from the First GENERATE AC Command Data using the *First GENERATE AC Unchanging Log Data Table*	if any
Data Extracted from the Second GENERATE AC Command Data using the *Second GENERATE AC Log Data Table*	if any
Additional card data	if Internal Data Logging implementer-option is supported and *Internal Log Data Object List (ILDOL)* is present

Table 18: Transaction Log Entry for Second GENERATE AC Logging

13.2.9.3 Return GENERATE AC Response

Section 17.5.8.4 of [CPA] is replaced with the following text.

Req C.122 Data field in second GENERATE AC response message

The data field in the second GENERATE AC response message returned by the CPACE application shall be coded

- as shown in Table 19, if no CDA signature is returned,
- as shown in Table 20, if a CDA signature is returned.

Tag	Value		Presence
'77'	*Response Message Template Format 2*		M
	'9F27'	*Cryptogram Information Data (CID)*	M
	'9F36'	*Application Transaction Counter (ATC)*	M
	'9F26'	*Application Cryptogram (AC)*	M
	'9F10'	*Issuer Application Data (IAD)*	M

Table 19: Second GENERATE AC Response Message Data Field - No CDA

Tag	Value		Presence
'77'	*Response Message Template Format 2*		M
	'9F27'	*Cryptogram Information Data (CID)*	M
	'9F36'	*Application Transaction Counter (ATC)*	M
	'9F4B'	*Signed Dynamic Application Data (SDAD)*	M
	'9F10'	*Issuer Application Data (IAD)*	M

Table 20: Second GENERATE AC Response Message Data Field - CDA

Req C.123 Generate CDA signature on TC if requested

If **both** of the following are true:

- CDA processing is requested by the terminal (that is, 'CDA Requested' in the P1 parameter in the GENERATE AC command from the terminal was set to 1b),
- **and** the CPACE application is responding with a TC type *Application Cryptogram*,

then the CPACE application

- shall generate a dynamic signature as described in Section 6.6.1 of [EMV 2], including the tags, lengths, and values of the data elements returned in the *Response Message Template Format 2* shown in Table 20 in the order they are returned, with the exception of the *Signed Dynamic Application Data*,
- shall return a second GENERATE AC response with a response message data field shown in Table 20.

Otherwise, the CPACE application shall return a second GENERATE AC response with a response message data field shown in Table 19.

14 Issuer Script Command Processing

14.1 Introduction

This section refers to Section 18 of [CPA]:

- A modification regarding Section 18.5.3.1 of [CPA] (Message Authentication (MACing)) is described in Section 14.2.
- An additional requirement regarding Section 18.5.5 of [CPA] (Script Commands Supported) is described in Section 14.3.
- A modification regarding Section 18.8 of [CPA] (PUT DATA Command) is described in Section 14.4.
- Additional requirements and additional text regarding Section 18.9.1.1 of [CPA] (UPDATE RECORD Command Format Validation) are described in Section 14.5.1.
- Additional requirements and additional text regarding Section 18.9.2 of [CPA] (UPDATE RECORD Processing) are described in Section 14.5.2.
- The additional script commands ACTIVATE CL Command and DEACTIVATE CL Command are described in Sections 14.6 and 14.7. The unsecured DEACTIVATE CL Command is described in Section 14.7 too.

  Sections 14.6 and 14.7 are additional sub-sections of Section 18 of [CPA]. The general requirements described in Section 18.5 of [CPA] also apply to the ACTIVATE CL Command and DEACTIVATE CL Command.

14.2 Message Authentication (MACing)

Req 18.3 and the following Note in Section 18.5.3.1 of [CPA] are replaced with the following requirement.

Req C.124	**Message Authentication (MACing)**
The CPACE application shall support 4-byte MACs. If the Other MAC Lengths implementer-option is supported the CPACE application shall support MACs of length 4 to 8 bytes.	

14.3 Script Commands Supported

The following text and requirement are added at the end of Section 18.5.5 of [CPA].

According to this specification, script commands may be used by the issuer to activate or deactivate contactless access to the CPACE dual interface card when the Contactless Control - Card implementer-option is supported or to activate or deactivate contactless access to the CPACE application on a dual interface card when the Contactless Control - Application implementer-option is supported.

Req C.125	**Additional supported script commands**
If the Contactless Control - Card implementer-option is supported or if the Contactless Control - Application implementer-option is supported, then the CPACE card shall support the following additional script commands (see Req C.26): • ACTIVATE CL command as specified in Section 14.6 • DEACTIVATE CL script command as specified in Section 14.7. If the Contactless Control - Card implementer-option is supported or if the Contactless Control - Application implementer-option is supported, then the CPACE application shall also support the unsecured DEACTIVATE script command as specified in Section 14.7.	

14.4 PUT DATA Command

Req 18.30 in Section 18.8 of [CPA] is replaced with the following requirement.

Req C.126	**Data elements supported by PUT DATA**
Table J-1 in Annex J of [CPA] and Table 40 in Section 19 show the only EMV-defined and CPACE-defined application data elements and templates that may be updated using the PUT DATA command.	

14.5 UPDATE RECORD Command

14.5.1 UPDATE RECORD Command Format Validation

The paragraph between Req 18.45 and Req 18.46 in Section 18.9.1.1 of [CPA] is replaced with the following requirements and text.

Req C.127	**UPDATE RECORD supported for *AID-Interface Entries***
The AID-Interface File shall be updateable with the UPDATE RECORD command.	

Req C.128	**UPDATE RECORD supported for *RRP Configuration Data Sets***
The RRP Configuration File shall be updateable with the UPDATE RECORD command.	

The use of files that are not EMV files, payment system-specific files, the Transaction Log file, the file containing the *Profile Selection Entries*, the AID-Interface File or the RRP Configuration File is permitted as additional functionality (for instance, issuer-specific files), but is beyond the scope of this specification. Support for these files by the UPDATE RECORD command is also beyond the scope of this specification.

14.5.2 UPDATE RECORD Processing

The two paragraphs preceding Req 18.52 in Section 18.9.2 of [CPA] are replaced with the following text.

For records containing the *Profile Selection Entries*, for records containing the *AID-Interface Entries* and for records containing the *RRP Configuration Data Set*s; because the UPDATE RECORD command has a length for the command data in addition to the length of the *Profile Selection Entry*, the *AID-Interface Entry* or *RRP Configuration Data Set* contained in the record, the issuer is allowed to add filler bytes to the end of the *Profile Selection Entry*, *AID-Interface Entry* or *RRP Configuration Data Set* in a record. To ensure that the *Profile Selection Entry*, *AID-Interface Entry* and *RRP Configuration Data Set* can be correctly processed by the application, if filler bytes are added, they should be added to the end of the *Profile Selection Entry*, *AID-Interface Entry* or *RRP Configuration Data Set*.

NOTE: EMV uses the value '00' for filler bytes.

The paragraph between Req 18.52 und Req 18.53 in Section 18.9.2 of [CPA] is replaced with the following requirements and text.

Req C.129	**Filler bytes not required in UPDATE RECORD to *AID-Interface Entry***
The UPDATE RECORD command shall accept *AID-Interface Entry* records without filler bytes.	

Req C.130	**Filler bytes not required in UPDATE RECORD to *RRP Configuration Data Set***
The UPDATE RECORD command shall accept *RRP Configuration Data Set* records without filler bytes.	

The UPDATE RECORD command to a *Profile Selection Entry*, an *AID-Interface Entry* or *RRP Configuration Data Set* is allowed to contain trailing filler bytes of value '00'.

14.6 ACTIVATE CL Command

The ACTIVATE CL Command may be used by the issuer during Issuer-to-Card Script Processing to activate contactless access to the CPACE dual interface card when the Contactless Control - Card implementer-option is supported or to activate contactless access to the CPACE application on a dual interface card when the Contactless Control - Application implementer-option is supported.

Processing of the ACTIVATE CL Command described in this section, only applies if the Contactless Control - Card implementer-option is supported or if the Contactless Control - Application implementer-option is supported.

Since support of the Contactless Control - Card implementer-option implies support of the Contactless Control - Application implementer-option, it is assumed without mentioning in this section, that the Contactless Control - Application implementer-option is supported.

Only if support of the Contactless Control - Card implementer-option is relevant for processing of the ACTIVATE CL Command, this is mentioned as a condition in the respective requirements in this section.

14.6.1 ACTIVATE CL Command Coding

The ACTIVATE CL command message is coded as follows:

Code	Value
CLA	'EC'
INS	'44'
P1	See Table 22
P2	'00'
Lc	Length of Secure Messaging Data
Data	Secure Messaging Data
Le	Not present

Table 21: ACTIVATE CL Command Message

Coding of P1:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	-	x	Apply activation of contactless access to
-	-	-	-	-	-	-	0	APPLICATION
-	-	-	-	-	-	-	1	CARD
x	x	x	x	x	x	x	-	RFU

Table 22: Coding of P1 for ACTIVATE CL

Req C.131	**ACTIVATE CL script command received**
If the application receives the ACTIVATE CL command (always CLA = 'EC'), then the application shall set the 'Script received' bit in the *PTH* to the value 1b.	

14.6.2 ACTIVATE CL Command Format Validation

Req C.132	**Check P1 value for ACTIVATE CL command**

If **either** of the following is true:

- P2 is set to a value other than '00' or '01',
- **or both** of the following are true:
  - the Contactless Control - Card implementer-option is not supported,
  - **and** P1 is set to the value '01'

then the CPACE application:

- shall set the 'Script failed' bit in *PTH* to the value 1b,
- shall discontinue processing the ACTIVATE CL command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6A86' (Incorrect Parameters, P1-P2).

Req C.133	**Check P2 value for ACTIVATE CL command**

If P2 is set to a value other than '00' then the CPACE application:

- shall set the 'Script failed' bit in *PTH* to the value 1b,
- shall discontinue processing the ACTIVATE CL command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6A86' (Incorrect Parameters, P1-P2).

14.6.3 ACTIVATE CL Command Processing

The command data (Secure Messaging Data) contains only the MAC data object:

Tag	Length	Value
'8E'	'04' - '08'	MAC

Req C.134	**Check MAC tag**

If the first byte of the command data has a value other than '8E' (MAC tag), then the CPACE application:

- shall set the 'Script failed' bit in *PTH* to the value 1b,
- shall discontinue processing the ACTIVATE CL command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6987' (Expected secure messaging data objects missing).

Req C.135	**Check MAC length**

If the second byte of the command data has a value other than Lc - 2, then the CPACE application:

- shall set the 'Script failed' bit in *PTH* to the value 1b,
- shall discontinue processing the ACTIVATE CL command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6988' (Incorrect secure messaging data objects).

The application verifies the MAC.

Req C.136	**Verify MAC**

If the MAC verification is not successful, then the CPACE application:

- shall set the 'Script failed' bit in *PTH* to the value 1b,
- shall discontinue processing the ACTIVATE CL command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6982' (Security status not satisfied).

Req C.137	**Activate contactless access and finalise processing**

If the MAC verification is successful, then the CPACE application shall:

- activate contactless access to the CPACE card according to Req C.138
- activate contactless access to the CPACE application according to Req C.139
- increment by one the Issuer Script Command Counter
- respond with SW1 SW2 = '9000'

Req C.138	**Activate contactless access to card - ACTIVATE CL**

If **all** of the following are true:

- the Contactless Control - Card implementer-option is supported,
- **and** 'Right of application to activate/deactivate contactless access to the card' in *Contactless Control - Application* = ENABLED,
- **and** 'Apply activation of contactless access to' in P1 = CARD,
- **and** *Contactless Control - Card* is present in the CPACE card,

then the following steps shall be performed:

- 'State of contactless access to the card' in *Contactless Control - Card* shall be set to ACTIVATED,
- 'Enablement of unsecured DEACTIVATE CL command for the card' in *Contactless Control - Card* shall be set to DISABLED.

Note:

If *Contactless Control - Application* is not present in the CPACE application, then the CPACE application shall use the value '80' (see Section 16.7). In this case contactless access to the CPACE card will remain unchanged.

Req C.139	**Activate contactless access to application - ACTIVATE CL**

If **both** of the following are true:

- 'Apply activation of contactless access to' in P1 = APPLICATION,
- **and** *Contactless Control - Application* is present in the CPACE application,

then the following steps shall be performed:

- 'State of contactless access to the application' in *Contactless Control - Application* shall be set to ACTIVATED,
- 'Enablement of unsecured DEACTIVATE CL command for the application' in *Contactless Control - Application* shall be set to DISABLED.

14.7 DEACTIVATE CL Command

The DEACTIVATE CL Command may be used by the issuer during Issuer-to-Card Script Processing to deactivate contactless access to the CPACE dual interface card when the Contactless Control - Card implementer-option is supported or to deactivate contactless access to the CPACE application on a dual interface card when the Contactless Control - Application implementer-option is supported.

In addition, if the Contactless Control - Card implementer-option is supported or if the Contactless Control - Application implementer-option is supported, for testing purposes during card personalisation, after performing tests on the contact or contactless interface, the unsecured DEACTIVATE CL Command can be used to put the CPACE card or application (back) to the state where contactless access is deactivated.

Processing of the DEACTIVATE CL Command described in this section, only applies if the Contactless Control - Card implementer-option is supported or if the Contactless Control - Application implementer-option is supported.

Since support of the Contactless Control - Card implementer-option implies support of the Contactless Control - Application implementer-option, it is assumed without mentioning in this section, that the Contactless Control - Application implementer-option is supported.

Only if support of the Contactless Control - Card implementer-option is relevant for processing of the DEACTIVATE CL Command, this is mentioned as a condition in the respective requirements in this section.

14.7.1 DEACTIVATE CL Command Coding

The DEACTIVATE CL script command message is coded as follows:

Code	Value
CLA	'EC'
INS	'04'
P1	See Table 25
P2	See Table 26
Lc	Length of Secure Messaging Data
Data	Secure Messaging Data
Le	Not present

Table 23: DEACTIVATE CL Script Command Message

The unsecured DEACTIVATE CL command message is coded as follows:

Code	Value
CLA	'E0'
INS	'04'
P1	See Table 25
P2	See Table 26
Lc	Not present
Data	Not present
Le	Not present

Table 24: Unsecured DEACTIVATE CL Command Message

Coding of P1:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	-	x	Apply deactivation of contactless access to
-	-	-	-	-	-	-	0	APPLICATION
-	-	-	-	-	-	-	1	CARD
x	x	x	x	x	x	x	-	RFU

Table 25: Coding of P1 for DEACTIVATE CL

Coding of P2:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	-	x	Disable unsecured DEACTIVATE CL
-	-	-	-	-	-	-	0	DO NOT DISABLE
-	-	-	-	-	-	-	1	DISABLE
x	x	x	x	x	x	x	-	RFU

Table 26: Coding of P2 for unsecured DEACTIVATE CL

Req C.140 DEACTIVATE CL script command received

If the application receives the DEACTIVATE CL script command (only if CLA = 'EC'), then the application shall set the 'Script received' bit in the *PTH* to the value 1b.

14.7.2 DEACTIVATE CL Command Format Validation

Req C.141 Check P1 value for DEACTIVATE CL command

If **either** of the following is true:

- P1 is set to a value other than '00' or '01',
- **or both** of the following are true:
  - the Contactless Control - Card implementer-option is not supported,
  - **and** P1 is set to the value '01'

then the CPACE application:

- shall set the 'Script failed' bit in *PTH* to the value 1b, only if CLA = 'EC',
- shall discontinue processing the DEACTIVATE CL command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6A86' (Incorrect Parameters, P1-P2).

Req C.142	**Check P2 value for DEACTIVATE CL command**

If P2 is set to a value other than '00' or '01', then the CPACE application:

- shall set the 'Script failed' bit in *PTH* to the value 1b, only if CLA = 'EC',
- shall discontinue processing the DEACTIVATE CL command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6A86' (Incorrect Parameters, P1-P2).

14.7.3 DEACTIVATE CL Command Processing

If CLA = 'EC' the command data (Secure Messaging Data) contains only the MAC data object:

Tag	Length	Value
'8E'	'04' - '08'	MAC

Req C.143	**Check MAC tag**

If CLA = 'EC' and if the first byte of the command data has a value other than '8E' (MAC tag), then the CPACE application:

- shall set the 'Script failed' bit in *PTH* to the value 1b,
- shall discontinue processing the DEACTIVATE CL command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6987' (Expected secure messaging data objects missing).

Req C.144	**Check MAC length**

If CLA = 'EC' and if the second byte of the command data has a value other than Lc - 2, then the CPACE application:

- shall set the 'Script failed' bit in *PTH* to the value 1b,
- shall discontinue processing the DEACTIVATE CL command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6988' (Incorrect secure messaging data objects).

If CLA = 'EC', then the application verifies the MAC.

Req C.145	**Verify MAC**

If CLA = 'EC' and if the MAC verification is not successful, then the CPACE application:

- shall set the 'Script failed' bit in *PTH* to the value 1b,
- shall discontinue processing the DEACTIVATE CL command, shall respond with an SW1 SW2 that indicates an error, and should respond with SW1 SW2 = '6982' (Security status not satisfied).

Req C.146	**Deactivate contactless access and finalise processing**

If either of the following is true:

- CLA = 'EC' and the MAC verification is successful,
- or CLA = 'E0'

then the CPACE application shall:

- deactivate contactless access to the CPACE card according to Req C.147
- deactivate contactless access to the CPACE application according to Req C.148
- increment by one the Issuer Script Command Counter, if CLA = 'EC'
- respond with SW1 SW2 = '9000'

Req C.147	**Deactivate contactless access to card - DEACTIVATE CL**

If **all** of the following are true:

- the Contactless Control - Card implementer-option is supported,
- **and** 'Right of application to activate/deactivate contactless access to the card' in *Contactless Control - Application* = ENABLED,
- **and** 'Apply deactivation of contactless access to' in P1 = CARD,
- **and** *Contactless Control - Card* is present in the CPACE card,
- **and either** of the following is true:
  - CLA = 'EC',
  - **or both** of the following are true:
    - CLA = 'E0',
    - **and any** of the following is true:
      - 'Enablement of unsecured DEACTIVATE CL command for the card' in *Contactless Control - Card* = ENABLED FOR CONTACT AND CONTACTLESS,

- **or both** of the following are true:
  - 'Enablement of unsecured DEACTIVATE CL command for the card' in *Contactless Control - Card* = ENABLED FOR CONTACT,
  - **and** the interface in use is contact,
- **or both** of the following are true:
  - 'Enablement of unsecured DEACTIVATE CL command for the card' in *Contactless Control - Card* = ENABLED FOR CONTACTLESS,
  - **and** the interface in use is contactless,

then the following steps shall be performed:

- 'State of contactless access to the card' in *Contactless Control - Card* shall be set to DEACTIVATED,
- if (and only if) 'Disable unsecured DEACTIVATE CL' in P2 = DISABLE, then 'Enablement of unsecured DEACTIVATE CL command for the card' in *Contactless Control - Card* shall be set to DISABLED,
- if (and only if) CLA = 'EC', then:
  - 'Activation of contactless access to the card with SELECT of an application on the contact interface' in *Contactless Control - Card* shall be set to DISABLED,
  - 'Activation of contactless access to the card with successful VERIFY command on the contact interface' in *Contactless Control - Card* shall be set to DISABLED,
  - 'Activation of contactless access to the card with second GENERATE AC and successful Issuer Authentication on the contact interface' in *Contactless Control - Card* shall be set to DISABLED.

Note:

If *Contactless Control - Application* is not present in the CPACE application, then the CPACE application shall use the value '80' (see Section 16.7). In this case contactless access to the CPACE card will remain unchanged.

Req C.148 Deactivate contactless access to application - DEACTIVATE CL

If **all** of the following are true:

- 'Apply deactivation of contactless access to' in P1 = APPLICATION,
- **and** *Contactless Control - Application* is present in the CPACE application,
- **and either** of the following is true:
  - CLA = 'EC',
  - **or both** of the following are true:
    - CLA = 'E0',
    - **and any** of the following is true:
      - 'Enablement of unsecured DEACTIVATE CL command for the application' in *Contactless Control - Application* = ENABLED FOR CONTACT AND CONTACTLESS,
      - **or both** of the following are true:
        - 'Enablement of unsecured DEACTIVATE CL command for the application' in *Contactless Control - Application* = ENABLED FOR CONTACT,
        - **and** the interface in use is contact,
      - **or both** of the following are true:
        - 'Enablement of unsecured DEACTIVATE CL command for the application' in *Contactless Control - Application* = ENABLED FOR CONTACTLESS,
        - **and** the interface in use is contactless,

then the following steps shall be performed:

- 'State of contactless access to the application' in *Contactless Control - Application* shall be set to DEACTIVATED,
- if (and only if) 'Disable unsecured DEACTIVATE CL' in P2 = DISABLE, then 'Enablement of unsecured DEACTIVATE CL command for the application' in *Contactless Control - Application* shall be set to DISABLED,
- if (and only if) CLA = 'EC', then:
  - 'Activation of contactless access to the application with SELECT of the application on the contact interface' in *Contactless Control - Application* shall be set to DISABLED,
  - 'Activation of contactless access to the application with successful VERIFY command on the contact interface' in *Contactless Control - Application* shall be set to DISABLED,
  - 'Activation of contactless access to the application with second GENERATE AC and successful Issuer Authentication on the contact interface' in *Contactless Control - Application* shall be set to DISABLED.

15 Security and Key Management

15.1 Introduction

This section refers to Section 20 of [CPA]:

- Additional requirements regarding cryptographic keys and their usage are described in Section 15.2 (Cryptographic Keys), which is inserted as additional sub-section 20.0 before Section 20.1 of [CPA].
- An additional requirement regarding Section 20.5 of [CPA] (Other Data Requirements) and Specification Bulletin 165 is described in Section 15.3.

15.2 Cryptographic Keys

According to [CPA], storage of one set of symmetric master keys shall be supported per instance of the CPACE application. According to this specification, this set of master keys is called the standard set of symmetric master keys and it is referred to as *Standard Master Keys*. *Standard Master Keys* consists of the standard master keys *Master Key for AC*, *Master Key for SMC* and *Master Key for SMI* described in [CPA].

Note:

If the Cryptogram Version '5'-only implementer-option is supported, *Standard Master Keys* is a set of Triple DES keys, each with a length of 16 bytes.

If the Cryptogram Version '6'-only implementer-option is supported, *Standard Master Keys* is a set of AES keys each with the same length of either 16, 24 or 32 bytes.

If the Cryptogram Version '5' and '6' implementer-option is supported, the CPACE application shall allow personalising either Triple DES or AES versions of the master keys. Therefore, if the Cryptogram Version '5' and '6' implementer-option is supported, *Standard Master Keys* is either a set of Triple DES keys, each with a length of 16 bytes, or a set of AES keys each with the same length of either 16, 24 or 32 bytes.

The following requirement applies to the CPACE application if the Additional Master Keys implementer-option is supported.

Req C.149	**Support of additional symmetric master keys**

If the Additional Master Keys implementer-option is supported, then the CPACE application shall support storage of 15 additional sets of symmetric master keys, referred to as *Additional Master Keys x*, where x has a value between 1 and 15.

Each *Additional Master Keys x* consists of an *Additional Master Key for AC x*, an *Additional Master Key for SMC x* and an *Additional Master Key for SMI x*

It shall be an issuer option to personalise one or several of these additional sets of symmetric master keys.

If the Additional Master Keys implementer-option is supported, then the set of master keys to be used for a transaction is profile-specific. The set of master keys to be used is identified by the 'Master Keys ID' (bits b8-b5 of byte 7) in the *Profile Control*. The evaluation of the 'Master Keys ID' (bits b8-b5 of byte 7) in the *Profile Control* shall be performed as described in Req C.77.

If the Cryptogram Version '5'-only implementer-option is supported, *Additional Master Keys x* is a set of Triple DES keys, each with a length of 16 bytes.

If the Cryptogram Version '6'-only implementer-option is supported, *Additional Master Keys x* is a set of AES keys, each with the same length of either 16, 24 or 32 bytes.

If the Cryptogram Version '5' and '6' implementer-option is supported, *Additional Master Keys x* is either a set of Triple DES keys, each with a length of 16 bytes, or a set of AES keys, each with the same length of either 16, 24 or 32 bytes.

It is not required, that the CPACE application supports different key lengths for the *Additional Master Key for AC x*, the *Additional Master Key for SMC x* and the *Additional Master Key for SMI x* in a set of master keys *Additional Master Keys x*.

The following requirement applies to asymmetric cryptography supported by the CPACE application.

Req C.150	**Maximum RSA key length**

The CPACE implementation shall support the maximum RSA key lengths required for EMV processing within the EMV required performance (see Req C.21).

15.3 Other Data Requirements

The following requirement is appended after Req 20.14 (as replaced by Specification Bulletin 165) in Section 20.5 of [CPA].

Req C.151	**Enciphering Issuer Discretionary Data in *Issuer Application Data***

If the (14-byte) Issuer Discretionary Data (IDD) portion of the *Issuer Application Data* is to be enciphered **using AES**, then the IDD portion of the *Issuer Application Data* shall be enciphered as follows:

- The 14-byte IDD block shall be XORed with the leftmost 14 bytes of a 16-byte mask S.
- The mask S is a ciphertext computed as the encipherment of a 16-byte value '00..03' (15 bytes '00' followed by one byte '03') using AES in ECB Mode as defined in Appendix A1.1 of [EMV 2], with no additional padding applied (thus the ciphertext S is 16 bytes long):
  - S = AES(ECK)['00..03']
- The k-bit encipherment key (ECK) used shall be a variant of the k-bit AC session key (SK_{AC}) computed as follows:
  - ECK := SK_{AC} XOR ('59'||'00'||'00'|| … ||'00'||'00'||'00')

  with (k-8)/8 bytes of '00'.

16 Personalisation

16.1 Introduction

This section refers to Section 21 of [CPA]:

- Modifications regarding Section 21.1.2 (CPA Data Elements Requiring Personalisation) are described in Section 16.2.
- Additional requirements regarding Section 21.2.8 (CPA Recommended Data Group Indicators for Records) are described in Section 16.3.
- Additional requirements regarding Section 21.2.9 (DGIs for Internal Application Data) are described in Section 16.4.
- A modification regarding Section 21.2.10 (DGIs for Command Response Data) is described in Section 16.5.
- A modification regarding the Specification Bulletin 165 amendment to Section 21.2.11 (DGIs for PIN and Key Related Data) is described in Section 16.6.
- Additional and modified requirements regarding Section 21.4 (Missing Data Elements) are described in Section 16.7.

16.2 CPA Data Elements Requiring Personalisation

The first paragraph of Section 21.1.2 of [CPA] is replaced with the following text.

Any value of AID and FCI allowed by EMV may be chosen by the issuer for the AIDs assigned to the CPACE application. The FCI are personalised in *AID-Interface Entries* in records of the AID-Interface File. When EMV CPS is used, the AID-Interface File is personalised as described in Section 16.3.

The following row is appended at the end of Table 21-2 in Section 21.1.2 of [CPA].

Tag	Data Element Name	Size (bytes)	Format
'D6'	*AID-Interface File Entry*	2	binary

The following rows are appended at the end of Table 21-3 in Section 21.1.2 of [CPA].

Tag	Data Element Name	Condition	Size (bytes)	Format
'D4'	*Contactless Control - Application*	If Contactless Control - Application implementer-option supported and an issuer wants to deactivate contactless access to the application	1	binary
'D3'	*Contactless Control - Card*	If Contactless Control - Card implementer-option supported and an issuer wants to deactivate contactless access to the card	1	binary
'D1'	*Dynamic Issuer Data*	If an issuer chooses to personalise the data element with a specific value	var.	binary
'D0'	*Static Issuer Data*	If an issuer chooses to personalise the data element with a specific value	var.	binary
'D9'	*RRP Configuration File Entry*	If Relay Resistance Protocol implementer-option supported and an issuer chooses to support the Relay Resistance Protocol for one or more profile(s)	2	binary

Note:

Contactless Control - Card should be present only once per CPACE dual interface card. Therefore it is not necessary to personalise this data element for each CPACE application.

The following requirement and tables are inserted between Table 21-4 and Req 21.8 in Section 21.1.2 of [CPA].

Req C.152	**Personalisation of additional symmetric master keys**

If the Additional Master Keys implementer-option is supported and the issuer chooses to use one or several additional set(s) of symmetric master keys *Additional Master Keys x*, where x has a value between 1 and 15, then either the data elements listed in Table 27 or, if the Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option is supported, the data elements listed in Table 28 shall be personalised per *Additional Master Keys x*.

The value of x and the cryptographic algorithm associated with the master keys in *Additional Master Keys x* shall be identified during personalisation.

If the EMV CPS implementer-option is supported, then the DGIs used to personalise *Additional Master Keys x* indicate the value of x and the cryptographic algorithm associated with the master keys in *Additional Master Keys x*.

If the EMV CPS implementer-option is not supported, it is out of scope for this specification, how the value of x and the cryptographic algorithm associated with the master keys in *Additional Master Keys x* are identified.

If the Cryptogram Version '5'-only implementer-option is supported, then *Additional Master Keys x* shall be personalised with a set of Triple DES keys, each with a length of 16 bytes.

If the Cryptogram Version '6'-only implementer-option is supported, then *Additional Master Keys x* shall be personalised with a set of AES keys, each with the same length of either 16, 24 or 32 bytes.

If the Cryptogram Version '5' and '6' implementer-option is supported, then *Additional Master Keys x* shall be personalised either with a set of Triple DES keys, each with a length of 16 bytes, or with a set of AES keys, each with the same length of either 16, 24 or 32 bytes.

Template Tag	Tag #	Data Element Name	Size (bytes)	Format
-	-	*Additional Master Key for AC x* (Triple DES)	16	binary
-	-	*Additional Master Key for SMC x* (Triple DES)	16	binary
-	-	*Additional Master Key for SMI x* (Triple DES)	16	binary

Table 27: CPACE Persistent Data Elements - Issuer-optional Additional Master Keys Option Elements - Triple DES

Template Tag	Tag #	Data Element Name	Size (bytes)	Format
-	-	*Additional Master Key for AC x* (AES)	16, 24, 32	binary
-	-	*Additional Master Key for SMC x* (AES)	16, 24, 32	binary
-	-	*Additional Master Key for SMI x* (AES)	16, 24, 32	binary

Table 28: CPACE Persistent Data Elements - Issuer-optional Additional Master Keys Option Elements - AES

The following row is appended at the end of Table 21-5 in Section 21.1.2 of [CPA].

Template Tag	Tag #	Data Element Name	Size (bytes)	Format
'BF40'	'DF05'	*Internal Log Data Object List (ILDOL)*	variable	binary

The following requirement and table are inserted between Table 21-5 and Req 21.9 in Section 21.1.2 of [CPA].

Req C.153	**Personalisation of command access control data**
If the Contactless Command Access Controls implementer-option is supported, then it shall be an issuer option to personalise any of the data elements listed in Table 29.	

Template Tag	Tag #	Data Element Name	Size (bytes)	Format
'E0'	'DF01'	*Contactless Command Access*	2	binary
'E0'	'DF02'	*Contactless READ RECORD Access*	var.	binary
'E0'	'DF03'	*Contactless GET DATA Access*	var.	binary

Table 29: Unique CPACE Persistent Data Elements - Issuer-optional Contactless Command Access Controls Option Elements

Req 21.9 and Table 21-6 in Section 21.1.2 of [CPA] are replaced with the following text.

Req C.154	**Personalisation of optional security data**
If the Application Security Counters implementer-option (see Section 18) is supported, then *Security Limits* in Table 30 shall be personalised. If the Additional Master Keys implementer-option (see Section 15.2) and the Application Security Counters implementer-option (see Section 18) are supported, then *Additional Security Limits x* in Table 30 shall be personalised for each additional set of symmetric master keys *Additional Master Keys x* stored in the CPACE application.	

Template Tag	Tag #	Data Element Name	Size (bytes)	Format
-	'C5'	*Security Limits*	6	binary
'E2'	'DF01' - 'DF0n'	*Additional Security Limits x*	N*7	binary

Table 30: Unique CPACE Persistent Data Elements - Optional Security Limit Elements

The following rows are inserted at the beginning of Table 21-9 in Section 21.1.2 of [CPA].

Template Tag	Tag #	Data Element Name	Condition	Size (bytes)	Format
-	-	*AID-Interface Entries*	Always	var.	records
-	-	*RRP Configuration Data Sets*	If the Relay Resistance Protocol implementer-option is supported and the Relay Resistance Protocol is supported for at least one profile	6	records

The following rows of Table 21-9 in Section 21.1.2 of [CPA] are modified as shown.

Template Tag	Tag #	Data Element Name	Condition	Size (bytes)	Format
'BF31'	'DF01' - 'DF0n'	*Accumulator Profile Controls*	Always (at least one)	N*5 or N*6	binary
'BF32'	'DF01' - 'DF0n'	*Accumulator Controls*	Always (at least one)	N*6 or N*7	binary
'BF36'	'DF01' - 'DF0n'	*Counter Profile Controls*	Always (at least one)	N*4 or N*5	binary
'BF37'	'DF01' - 'DF0n'	*Counter Controls*	Always (at least one)	N*4 or N*5	binary
'BF3B'	'DF01' - 'DF0n'	*Issuer Options Profile Controls*	Always (at least one)	N*10 or N*13	binary
'BF3F'	'DF01' - 'DF0n'	*Profile Controls*	Always (at least one)	N*11 or N*13	binary

16.3 CPA Recommended Data Group Indicators for Records

The following text is appended at the end of Section 21.2.8 of [CPA].

For DGIs with the first byte equal to 'uu', where 'uu' is the value of the first byte of *AID-Interface File Entry*; the first byte indicates the SFI in which the data is to be stored, and the second byte indicates the record number within the SFI. 'uu' ranges in value from '15' to '1E', and 'tt' ranges in value from '01' to '10'.

Req.	Tag	Data Element	Length	Encrypt
M	-	*AID-Interface Entry* 'tt'	var.	No

Table 31: Data Content for DGI 'uutt'

Note:

Transaction logging requires tag '9F4D' in template tag 'BF0C' which is personalised as part of the *FCI Proprietary Template* in *AID-Interface Entry* 'tt'

For DGIs with the first byte equal to 'ww', where 'ww' is the value of the first byte of *RRP Configuration File Entry*; the first byte indicates the SFI in which the data is to be stored, and the second byte indicates the record number within the SFI. 'ww' ranges in value from '15' to '1E', and 'vv' ranges in value from '01' to the value of the second byte of *RRP Configuration File Entry*.

Req.	Tag	Data Element	Length	Encrypt
C	-	*RRP Configuration Data Set* 'vv'	6	No

Table 32: Data Content for DGI 'wwvv'

16.4 DGIs for Internal Application Data

The following rows are appended at the end of Table 21-26 in Section 21.2.9 of [CPA].

DGI	Description	Table	Encrypt	Defined
'4000'	Template 'E0', *Contactless Command Access Controls*	-	No	CPACE
'4002'	Template 'E2', *Additional Security Limits*	-	No	CPACE

The following rows are appended at the end of Table 21-27 in Section 21.2.9 of [CPA].

Req.	Tag	Data Element	Length	Encrypt
M	'D6'	*AID-Interface File Entry*	2	N/A
O	'D4'	*Contactless Control - Application*	1	N/A
O	'D3'	*Contactless Control - Card*	1	N/A
O	'D1'	*Dynamic Issuer Data*	var.	N/A
O	'D0'	*Static Issuer Data*	var.	N/A
C	'D9'	*RRP Configuration File Entry*	2	N/A

16.5 DGIs for Command Response Data

Section 21.2.10 of [CPA] is replaced with the following text.

SELECT response data for CPACE does not use DGI '9102' as defined in EMV CPS. Instead, the response to the SELECT command is built using the *AID-Interface Entry* in a record of the AID-Interface File which is personalised using DGI 'uutt' (see Section 16.3).

GET PROCESSING OPTIONS (GPO) response data for CPA uses DGI 'BF41' rather than DGI '9104' as defined in EMV CPS.

The values needed by the application to build the Issuer Application Data contained in the GENERATE AC command response is personalised using tag '9F10' in DGI '3000'.

16.6 DGIs for PIN and Key Related Data

The modification of Section 21.2.11 of [CPA] described in Specification Bulletin 165 is replaced with the following text.

If the Cryptogram Version '5'-only implementer-option is supported, *Standard Master Keys* is a set of Triple DES keys, each with a length of 16 bytes.

If the Cryptogram Version '6'-only implementer-option is supported, *Standard Master Keys* is a set of AES keys, each with the same length of either 16, 24 or 32 bytes.

If the Cryptogram Version '5' and '6' implementer-option is supported, *Standard Master Keys* is either a set of Triple DES keys, each with a length of 16 bytes, or a set of AES keys, each with the same length of either 16, 24 or 32 bytes.

If the Cryptogram Version '5'-only implementer-option and the Additional Master Keys implementer-option are supported, each *Additional Master Keys x* is a set of Triple DES keys, each with a length of 16 bytes.

If the Cryptogram Version '6'-only implementer-option and the Additional Master Keys implementer-option are supported, each *Additional Master Keys x* is a set of AES keys, each with the same length of either 16, 24 or 32 bytes.

If the Cryptogram Version '5' and '6' implementer-option and the Additional Master Keys implementer-option are supported, each *Additional Master Keys x* is either a set of Triple DES keys, each with a length of 16 bytes, or a set of AES keys, each with the same length of either 16, 24 or 32 bytes.

DGIs '8000' (Triple DES Keys, see Table 33) and '9000' (Triple DES Key Check Values, see Table 34) as defined in [CPS] are used to personalise the Triple DES *Standard Master Keys*.

DGIs '8002' (AES Keys, see Table 35) and '9002' (AES Key Check Values, see Table 36) defined in Specification Bulletin 165 are used to personalise the AES *Standard Master Keys*.

DGIs '840x' (Triple DES Keys, see Table 33) and '940x' (Triple DES Key Check Values, see Table 34) defined by this specification are used to personalise the Triple DES *Additional Master Keys x*.

DGIs '841x' (AES Keys, see Table 35) and '941x' (AES Key Check Values, see Table 36) defined by this specification are used to personalise the AES *Additional Master Keys x*.

Tag	Data Element	Length	Encrypt
N/A	*Master Key for AC* (Triple DES)	16	SKU_{DEK}
	Master Key for SMI (Triple DES)	16	
	Master Key for SMC (Triple DES)	16	

Table 33: Data Content for DGI '8000' and '840x'

Tag	Data Element	Length	Encrypt
N/A	Key Check Values for the card keys *Master Key for AC* (Triple DES),*Master Key for SMI* (Triple DES), *Master Key for SMC* (Triple DES)	9	N/A

Table 34: Data Content for DGI '9000' and '940x'

Tag	Data Element	Length	Encrypt
N/A	*Master Key for AC* (AES)	16, 24, 32	SKU_{DEK}
	Master Key for SMI (AES)	16, 24, 32	
	Master Key for SMC (AES)	16, 24, 32	

Table 35: Data Content for DGI '8002' and '841x'

Tag	Data Element	Length	Encrypt
N/A	Key Check Values for the card keys *Master Key for AC* (AES),*Master Key for SMI* (AES), *Master Key for SMC* (AES)	9	N/A

Table 36: Data Content for DGI '9002' and '941x'

The Key Check Value for any Triple DES key will be computed by encrypting 8 bytes of '00' using ECB Triple DES with the key concerned. The Key Check Value is the three leftmost bytes of the result.

The Key Check Value for any AES key is computed by encrypting 16 bytes of '01' using ECB AES with the key concerned. The Key Check Value is the three leftmost bytes of the result.

16.7 Missing Data Elements

The following requirements are inserted between the first paragraph and Req 21.49 in Section 21.4 of [CPA].

Req C.155	**Missing *Contactless Control - Application***
If the Contactless Control - Application implementer-option is supported, but the *Contactless Control - Application* is not present in the CPACE application, then the CPACE application shall use the value '80' for *Contactless Control - Application*, which activates contactless access, disables unsecured DEACTIVATE CL, disables implicit activation of contactless access and denies the right to activate/deactivate contactless access to the card for the CPACE application.	

Req C.156	**Missing *Contactless Control - Card***
If the Contactless Control - Card implementer-option is supported, but the *Contactless Control - Card* is not present in the CPACE card, then the CPACE application shall use the value '80' for *Contactless Control - Card*, which activates contactless access, disables unsecured DEACTIVATE CL and disables implicit activation of contactless access for the CPACE card.	

The following requirement is inserted between Req 21.51 and Req 21.52 in Section 21.4 of [CPA].

Req C.157	**Missing *Additional Master Keys x***
If **all** of the following are true: • the Additional Master Keys implementer-option is supported, • **and** 'Master Keys ID' (bits b8-b5 of byte 7) in the *Profile Control* has a value different from '0', • **and** *Additional Master Keys x*, where x has the value of 'Master Keys ID', is not present in the CPACE application then the CPACE application shall discontinue processing the GENERATE AC command and should respond with SW1 SW2 = '6985' (Conditions of use not satisfied).	

Req 21.64 in Section 21.4 of [CPA] is replaced by the following Req C.158.

Req C.158	**Missing *Issuer Options Profile Control***
If *Issuer Options Profile Control x* is not present in the application (where x is value of the Issuer Options Profile Control ID in the *Profile Control* selected for the transaction), then the CPACE application shall discontinue processing the GET PROCESSING OPTIONS command or the GENERATE AC command, and shall respond with SW1 SW2 = '6985' (Conditions of use not satisfied).	

17 Transaction Logging

17.1 Introduction

This section refers to Annex D of [CPA]:

- A modification regarding Annex D1 of [CPA] (Transaction Log Entry Description) is described in Section 17.2.
- New requirements regarding transaction logging using the *Internal Log Data Object List (ILDOL)* are described in Section 17.3.
- Modifications regarding Annex D4 of [CPA] (First GENERATE AC Transaction Logging and Second GENERATE AC Transaction Logging) are described in Section 17.4.

17.2 Transaction Log Entry Description

The following row is appended at the end of Table D-1 in Annex D1 of [CPA].

Optional additional card data Note: If the Internal Data Logging implementer-option is not supported or if the *Internal Log Data Object List (ILDOL)* is not present in the *Log Data Tables*, then no optional additional card data is logged for the transaction.	Additional card data	List of data elements identified by the *ILDOL*, built according to Section 5.4 of [EMV 3] using the current values of the data elements or binary zeroes.

17.3 *Internal Log Data Object List (ILDOL)*

If the Internal Data Logging implementer-option is supported, according to this specification, the issuer has the additional option to use the *Internal Log Data Object List (ILDOL)* to specify whether and which additional card data shall be logged.

If the transaction is logged, regardless of whether the transaction is logged during processing of the first or second GENERATE AC command, if the *ILDOL* is present in the *Log Data Tables* template, the list of data elements identified by the *ILDOL*

- shall be built according to the rules specified in Section 5.4 of [EMV 3], using the current values of the data elements,
- shall be appended as additional card data to the transaction log record.

17.4 Processing Transaction Logging

Annex D4 of [CPA] is replaced with the following text.

Transaction logging occurs as follows:

- when the first GENERATE AC response is a TC or an AAC, prior to responding to the first GENERATE AC command,
- when the first GENERATE AC response is an ARQC,
  - if 'Log Online Requests' in *Application Control* has the value 1b, prior to responding to the first GENERATE AC command,
  - prior to responding to the second GENERATE AC command.

17.4.1 First GENERATE AC Transaction Logging

If the application responds with a TC/AAC and the issuer chooses to log such transactions, a record with the information listed in Table 37 is appended to the Transaction Log.

Data to Log	**Condition**
Amount, Authorised	always
Transaction Currency Code	always
Transaction Date	always
CVR	if 'Log the CVR' in *Application Control* = 1b
ATC	if 'Log the ATC' in *Application Control* = 1b
CID	if 'Log the CID' in *Application Control* = 1b
Profile ID	if 'Log the Profile ID' in *Application Control* = 1b
Data Extracted from the First GENERATE AC Command Data using the *First GENERATE AC Unchanging Log Data Table*	if any
Data Extracted from the First GENERATE AC Command Data using the *First GENERATE AC Log Data Table*	if any
Additional card data	if Internal Data Logging implementer-option is supported and *Internal Log Data Object List (ILDOL)* is present

Table 37: Data Logged at First GENERATE AC for a TC or AAC

If the application responds with an ARQC and the issuer chooses not to log such transactions for the first GENERATE AC command, the CPACE application temporarily saves the data listed in Table 38 so that it can be logged during second GENERATE AC transaction logging.

Data to Log	Condition
Amount, Authorised	if 'Amounts included in CDOL2' bit in *Application Control* = 0b
Transaction Currency Code	always
Transaction Date	always
Data Extracted from the First GENERATE AC Command Data using the *First GENERATE AC Unchanging Log Data Table*	if any
Environment in Use, *DF Name* returned in the response to the SELECT command	if Internal Data Logging implementer-option is supported, *Internal Log Data Object List (ILDOL)* is present, and tag of data element is in *ILDOL*

Table 38: Data Saved for Second GENERATE AC after an ARQC

17.4.2 Second GENERATE AC Transaction Logging

Prior to responding to the second Generate AC command, the CPACE application

- appends the data listed in Table 39 to the Transaction Log file, if 'Log Online Requests' in *Application Control* has the value 0b,
- replaces the most recent record of the Transaction Log file with the data listed in Table 39, if 'Log Online Requests' in *Application Control* has the value 1b.

Data to Log	Condition
Amount, Authorised	always
Transaction Currency Code	always
Transaction Date	always
CVR	if 'Log the CVR' in *Application Control* = 1b
ATC	if 'Log the ATC' in *Application Control* = 1b
CID	if 'Log the CID' in *Application Control* = 1b
Profile ID	if 'Log the Profile ID' in *Application Control* = 1b
Data Extracted from the First GENERATE AC Command Data using the *First GENERATE AC Unchanging Log Data Table*	if any
Data Extracted from the Second GENERATE AC Command Data using the *Second GENERATE AC Log Data Table*	if any

Data to Log	Condition
Additional card data	if Internal Data Logging implementer-option is supported and *Internal Log Data Object List (ILDOL)* is present

Table 39: Data Logged at Second GENERATE AC

18 Security Counters

18.1 Introduction

This section refers to Annex F of [CPA]:

- A modification regarding the first paragraphs in Annex F of [CPA] (General) is described in Section 18.2.
- A modification regarding Annex F1 of [CPA] (Symmetric Keys) are described in Section 18.3.

18.2 General

The last paragraph preceding Annex F1 in Annex F of [CPA] is replaced with the following text.

For forensic purposes it will be possible to determine if a security counter has reached its limit by interrogating either the *Security Limits Status* data element or, if the Additional Master Keys implementer-option is supported, the *Additional Security Limits Status* data element, both described in Section 21 of this specification.

18.3 Symmetric Keys

The first two paragraphs in Annex F1 of [CPA] are replaced with the following text.

The CPACE application is required to maintain session key counters and associated limits as specified in this section.

To support EMV common session key derivation, the CPACE application uses separate 2-byte counters, each with an associated limit, for each master key for Application Cryptogram generation and for each master key for Secure Messaging for Integrity stored in the CPACE application. These are

- *AC Session Key Counter* and *AC Session Key Counter Limit* used for the standard *Master Key for AC*,
- *SMI Session Key Counter* and *SMI Session Key Counter Limit* used for the standard *Master Key for SMI,*
- *Additional AC Session Key Counter x* and *Additional AC Session Key Counter Limit x* used for each *Additional Master Key for AC x*, if the Additional Master Keys implementer-option is supported,
- *Additional SMI Session Key Counter x* and *Additional SMI Session Key Counter Limit x* used for each *Additional Master Key for SMI x*, if the Additional Master Keys implementer-option is supported.

The remaining part of this section describes the usage of *AC Session Key Counter* with its limit and of *SMI Session Key Counter* with its limit. Usage of *Additional AC Session Key Counter x* with their respective limits is the same as usage of *AC Session Key Counter* with

its limit. Usage of *Additional SMI Session Key Counter x* with their respective limits is the same as usage of *SMI Session Key Counter* with its limit.

19 GET DATA and PUT DATA Data Elements

Table 40 lists the templates and data elements that are supported by the CPACE application for the GET DATA and PUT DATA commands, in addition to those listed in Table J-1 in Annex J of [CPA].

Data Element or Template	Tag	GET DATA	PUT DATA
Additional Security Limits	'E2'	N	Y (if Additional Master Keys and Application Security Counters supported)
Additional Security Limits Status	'D8'	Y (if Additional Master Keys and Application Security Counters supported)	N
AID-Interface File Entry	'D6'	Y	N
Contactless Command Access Controls	'E0'	Y (if Contactless Command Access Controls supported)	Y (if Contactless Command Access Controls supported)
Contactless Control - Application	'D4'	Y (if Contactless Control - Application supported)	Y (if Contactless Control - Application supported)
Contactless Control - Card	'D3'	Y (if Contactless Control - Card supported)	Y (if Contactless Control - Card supported)
Dynamic Issuer Data	'D1'	Y	Y
Static Issuer Data	'D0'	Y	Y
RRP Configuration File Entry	'D9'	Y (if Relay Resistance Protocol implementer-option supported)	N

Table 40: Additional GET DATA and PUT DATA Data Elements and Templates

20 Data Elements Tags

Table 41 lists the tags and template tags used by or stored in a CPACE application which are not listed in Annex K of [CPA]. The column "Condition" in Table 41 indicates if support of the respective template or data element is only required if a condition is met.

Data Element	Template or Tag	Source	Condition
Static Issuer Data	'D0'	Card	-
Dynamic Issuer Data	'D1'	Card	-
Contactless Control - Card	'D3'	Card	Contactless Control - Card implementer-option
Contactless Control - Application	'D4'	Card	Contactless Control - Application implementer-option
Environment in Use	'D5'	Card	Internal Data Logging implementer-option
AID-Interface File Entry	'D6'	Card	-
Additional Security Limits Status	'D8'	Card	Additional Master Keys and Application Security Counters implementer-options
RRP Configuration File Entry	'D9'	Card	Relay Resistance Protocol implementer-option supported
Contactless Command Access Controls	'E0'	Card	Contactless Command Access Controls implementer-option
Additional Security Limits	'E2'	Card	Additional Master Keys and Application Security Counters implementer-options

Table 41: Additional Data Element Tags

21 Data Dictionary

This section contains the description of templates and data elements which are used by or stored in a CPACE application and are either not described in [CPA] or modified with regard to [CPA]. These templates and data elements are listed in Table 42 and are described in more detail in the following sections. The column "Condition" in Table 42 indicates if support of (the modification of) the respective template or data element is only required if a condition is met.

Data Element Name	Condition	Template	Tag
AC Session Key Counter	Application Security Counters implementer-option	-	-
AC Session Key Counter Limit	Application Security Counters implementer-option	-	-
Accumulator Profile Control x	-	'BF31'	'DF0x'
Accumulator x Control	-	'BF32'	'DF0x'
Additional AC Session Key Counter x	Additional Master Keys and Application Security Counters implementer-options	-	-
Additional AC Session Key Counter Limit x	Additional Master Keys and Application Security Counters implementer-options	-	-
Additional Master Key for AC x	Additional Master Keys implementer-option, AES version only for Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option	-	-
Additional Master Key for SMC x	Additional Master Keys implementer-option, AES version only for Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option	-	-
Additional Master Key for SMI x	Additional Master Keys implementer-option, AES version only for Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option	-	-
Additional Master Keys x	Additional Master Keys implementer-option, AES versions only for Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option	-	-
Additional Security Limits	Additional Master Keys and Application Security Counters implementer-options	-	'E2'

Data Element Name	Condition	Template	Tag
Additional Security Limits x	Additional Master Keys and Application Security Counters implementer-options	'E2'	'DF0x'
Additional Security Limits Status	Additional Master Keys and Application Security Counters implementer-options	-	'D8'
Additional SMI Session Key Counter x	Additional Master Keys and Application Security Counters implementer-options	-	-
Additional SMI Session Key Counter Limit x	Additional Master Keys and Application Security Counters implementer-options	-	-
AID	-	-	'4F'
AID-Interface Entry	-	-	-
AID-Interface File Entry	-	-	'D6'
AIP/AFL Entry x	-	'BF41'	'DF0X'
Application Control	-	-	'C1'
Application Decisional Results (ADR)	-	-	-
Card Issuer Actions Codes Entry x (CIACs Entry x)	-	'BF34'	'DF0x'
Card Status Update (CSU)	-	-	-
Card Verification Results (CVR)	-	-	'9F52'
Contactless Command Access	Contactless Command Access Controls implementer-option	'E0'	'DF01'
Contactless Command Access Controls	Contactless Command Access Controls implementer-option	-	'E0'
Contactless Control - Application	Contactless Control - Application implementer-option	-	'D4'
Contactless Control - Card	Contactless Control - Card implementer-option	-	'D3'
Contactless READ RECORD Access	Contactless Command Access Controls implementer-option	'E0'	'DF02'
Contactless GET DATA Access	Contactless Command Access Controls implementer-option	'E0'	'DF03'
Counter Profile Control x	-	'BF36'	'DF0x'
Counter x Control	-	'BF37'	'DF0x'
Device Estimated Transmission Time For Relay Resistance R-APDU	Relay Resistance Protocol implementer-option	-	-
Device Relay Resistance Entropy	Relay Resistance Protocol implementer-option	-	-
Dynamic Issuer Data	-	-	'D1'

Data Element Name	Condition	Template	Tag
Environment in Use	Internal Data Logging implementer-option	-	'D5'
GPO Parameters x	-	'BF3E'	'DFxx'
Internal Flags	-	-	-
Internal Log Data Object List (ILDOL)	Internal Data Logging implementer-option	'BF40'	'DF05'
Issuer Authentication Data (IATD)	-	-	'91'
Issuer Options Profile Control	-	-	-
Issuer Options Profile Control x	-	'BF3B'	'DF0x'
Log Data Tables	Internal Data Logging implementer-option	-	'BF40'
Master Key for AC	AES version only for Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option	-	-
Master Key for SMC	AES version only for Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option	-	-
Master Key for SMI	AES version only for Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option	-	-
Max Time For Processing Relay Resistance APDU	Relay Resistance Protocol implementer-option	-	-
Min Time For Processing Relay Resistance APDU	Relay Resistance Protocol implementer-option	-	-
Profile Control	-	-	-
Profile Control x	-	'BF3F'	'DFxx'
Profile Selection Entry	-	-	-
Proprietary Authentication Data (PAD)	-	-	-
RRP Configuration Data Set	Relay Resistance Protocol implementer-option	-	-
RRP Configuration File Entry	Relay Resistance Protocol implementer-option	-	'D9'
RRP Counter	Relay Resistance Protocol implementer-option	-	-
RRP Dynamic Number	Relay Resistance Protocol implementer-option	-	-
RRP Transaction Data Set	Relay Resistance Protocol implementer-option	-	-

Data Element Name	Condition	Template	Tag
Security Limits	Application Security Counters implementer-option	-	'C5'
Security Limits Status	Application Security Counters implementer-option	-	'C4'
SMI Session Key Counter	Application Security Counters implementer-option	-	-
SMI Session Key Counter Limit	Application Security Counters implementer-option	-	-
Standard Master Keys	AES version only for Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option	-	-
Static Issuer Data	-	-	'D0'
Terminal Relay Resistance Entropy	Relay Resistance Protocol implementer-option	-	-
Terminal Risk Management Data	-	-	'9F1D'
Terminal Verification Results (TVR)	-	-	'95'
Third Party Data	-	'BF0C' or '70'	'9F6E'
Transaction CVM	-	-	-

Table 42: Additional and Modified Data Objects

21.1 *AC Session Key Counter*

Template: -
Tag: -
Length (in bytes): 2
Format: b

Description: *AC Session Key Counter* is supported when the Application Security Counters implementer-option is supported (see Section 18).

AC Session Key Counter is the internal counter defined in [CPA] that counts the AC session key derivations using *Master Key for AC* since the last successful validation of an ARPC with *Master Key for AC*.

21.2 *AC Session Key Counter Limit*

Template: -
Tag: -
Length (in bytes): 2
Format: b

Description: *AC Session Key Counter Limit* is supported when the Application Security Counters implementer-option is supported (see Section 18).

AC Session Key Counter Limit is the limit defined in [CPA] that limits the number of AC session key derivations using *Master Key for AC* since the last successful validation of an ARPC with *Master Key for AC*.

21.3 *Accumulator Profile Control x*

Template: 'BF31'
Tag: 'DF0x'
Length (in bytes): 2 **or 3**
Format: b

Description: *Accumulator Profile Control x* indicates the issuer's choice of data and behaviour to configure an Accumulator (1-3) within a Profile.

x may have any value between 1 and 14 and is coded in the second byte of the tag 'DF0x'.

Bytes 1 and 2 of *Accumulator Profile Control x* are defined by [CPA]. Byte 3 is defined by this specification.

If 'Allow Extended Controls' (byte 4, bit b1) in the *Application Control* of a CPACE application has the value 0b, every *Accumulator Profile Control x* of the application shall have a length of 2 bytes.

If 'Allow Extended Controls' in the *Application Control* of a CPACE application has the value 1b, every *Accumulator Profile Control x* of the application shall have a length of 2 or 3 bytes.

Accumulator Profile Control x is coded as shown in Table 43.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	-	-	-	-	-	-	-	Allow Accumulation
	0	-	-	-	-	-	-	-	Do not allow Accumulation[2)]
	1	-	-	-	-	-	-	-	Allow Accumulation
	-	1	-	-	-	-	-	-	Reset Accumulator with Online Response
	-	-	1	-	-	-	-	-	Send Accumulator in IAD
	-	-	-	x	-	-	-	-	Send Offline Balance
	-	-	-	0	-	-	-	-	Send Accumulator x Value
	-	-	-	1	-	-	-	-	Send Offline Balance x
	-	-	-	-	x	x	x	x	RFU
2	x	x	x	-	-	-	-	-	RFU
	-	-	-	x	-	-	-	-	Limit Set ID
	-	-	-	0	-	-	-	-	Use Limit Set 0
	-	-	-	1	-	-	-	-	Use Limit Set 1
	-	-	-	-	x	x	x	x	Currency Conversion Table ID
	-	-	-	-	1	1	1	1	Currency Conversion Not Allowed
3	x	x	x	x	x	x	x	-	RFU
	-	-	-	-	-	-	-	1	Reset Accumulator with Offline PIN Verification

Table 43: *Accumulator Profile Control x* Coding

[2)] This setting allows Velocity Checking for Accumulator x to include accumulators that cannot be increased in the profile selected for the transaction.

21.4 *Accumulator x Control*

Template: 'BF32'
Tag: 'DF0x'
Length (in bytes): 3 **or 4**
Format: b

Description: *Accumulator x Control* indicates the issuer's choice of data and behaviour to configure Accumulator x independently of a Profile.

x may have a value between 1 and 3 and is coded in the second byte of the tag 'DF0x'.

Bytes 1 to 3 of *Accumulator x Control* are defined by [CPA]. Byte 4 is defined by this specification.

If 'Allow Extended Controls' (byte 4, bit b1) in the *Application Control* of a CPACE application has the value 0b, every *Accumulator x Control* of the application shall have a length of 3 bytes.

If 'Allow Extended Controls' in the *Application Control* of a CPACE application has the value 1b, every *Accumulator x Control* of the application shall have a length of 3 or 4 bytes.

Accumulator x Control is coded as shown in Table 44.

A bit in the 'Include Based on Transaction CVM' bits (byte 4, bits b4-b1) in *Accumulator x Control* shall be set to the value 0b if and only if the transaction is to be accumulated when the Cardholder Verification Method (CVM) indicated by this bit is the *Transaction CVM*.

Note:

- The value 0000b of the 'Include Based on *Transaction CVM*' bits indicates that accumulation shall be performed irrespective of the *Transaction CVM*, that is, irrespective of whether and how cardholder verification was performed during the current transaction.
- The determination of the *Transaction CVM* is described in Section 12.2.3.2.

Position	**Data**	**Length** (in bytes)	**Format**	**Value**
Bytes 1 - 2	Accumulator Currency Code	2	n 3	Numeric Currency Code, in which the accumulator is managed, coded according to ISO 4217
Byte(s) 3 (- 4)	Accumulator Parameters	1 **or 2**	b	See Table 45

Table 44: *Accumulator x Control*

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	1	-	-	-	-	-	-	-	Include ARQC Transaction in CRM Test[3)]
	-	1	-	-	-	-	-	-	Include Offline Approvals[4)]
	-	-	x	x	x	x	x	x	RFU
2	1	-	-	-	-	-	-	-	Include Online Requests
	-	x	x	x	-	-	-	-	RFU
	-	-	-	-	x	x	x	x	Include Based on Transaction CVM
	-	-	-	-	0	-	-	-	Include if Transaction CVM is Offline PIN
	-	-	-	-	-	0	-	-	Include if Transaction CVM is Online PIN
	-	-	-	-	-	-	0	-	Include if Transaction CVM is Signature
	-	-	-	-	-	-	-	0	Include if Transaction CVM is No CVM

Table 45: Accumulator Parameters Coding

21.5 *Additional AC Session Key Counter x*

Template: -
Tag: -
Length (in bytes): 2
Format: b

Description: *Additional AC Session Key Counter x* is supported when the Additional Master Keys implementer-option (see Section 15.2) and the Application Security Counters implementer-option (see Section 18) are supported.

x may have a value between 1 and 15 and indicates *Additional Master Key for AC x*, to which *Additional AC Session Key Counter x* is assigned.

Additional AC Session Key Counter x is the internal counter defined by this specification that counts the AC session key derivations using *Additional Master Key for AC x* since the last successful validation of an ARPC with *Additional Master Key for AC x*.

Note:

Only the *Additional AC Session Key Counter x* assigned to the *Additional Master Key for AC x* which the issuer has chosen to personalise for the CPACE application are used.

3) This bit applies only if the 'Include Offline Approvals' bit is set to 1b.

4) If this bit has the value 0b, Accumulator x will accumulate only online transactions (which may be accumulated during processing of the first GENERATE AC command if the 'Include Online Requests' bit is set to 1b or when the Accumulator is updated during processing of the second GENERATE AC command).

21.6 *Additional AC Session Key Counter Limit x*

Template:	-
Tag:	-
Length (in bytes):	2
Format:	b
Description:	*Additional AC Session Key Counter Limit x* is supported when the Additional Master Keys implementer-option (see Section 15.2) and the Application Security Counters implementer-option (see Section 18) are supported. x may have a value between 1 and 15 and indicates *Additional Master Key for AC x*, to which *Additional AC Session Key Counter Limit x* is assigned. *Additional AC Session Key Counter Limit x* is the limit defined by this specification that limits the number of AC session key derivations using *Additional Master Key for AC x* since the last successful validation of an ARPC with *Additional Master Key for AC x*.

21.7 *Additional Master Key for AC x*

Template:	-
Tag:	-
Length (in bytes):	16, if the Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option is supported also 24 or 32
Format:	b
Description:	*Additional Master Key for AC x* is the master key for Application Cryptogram generation in the set of symmetric master keys *Additional Master Keys x*.

21.8 *Additional Master Key for SMC x*

Template:	-
Tag:	-
Length (in bytes):	16, if the Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option is supported also 24 or 32
Format:	b
Description:	*Additional Master Key for SMC x* is the master key for Secure Messaging for Confidentiality in the set of symmetric master keys *Additional Master Keys x*.

21.9 *Additional Master Key for SMI x*

Template:	-
Tag:	-
Length (in bytes):	16, if the Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option is supported also 24 or 32
Format:	b
Description:	*Additional Master Key for SMI x* is the master key for Secure Messaging for Integrity in the set of symmetric master keys *Additional Master Keys x*.

21.10 *Additional Master Keys x*

Template:	-
Tag:	-
Length (in bytes):	var.
Format:	b
Description:	*Additional Master Keys x* is a set of symmetric master keys stored in the CPACE application, consisting of an *Additional Master Key for AC x*, an *Additional Master Key for SMC x* and an *Additional Master Key for SMI x*. According to [CPA], the CPACE application shall support storage of one set of symmetric master keys. According to this specification, this set of master keys is called the standard set of symmetric master keys and it is referred to as *Standard Master Keys*. If the Additional Master Keys implementer-option is supported, then the CPACE application shall support storage of 15 additional sets of symmetric master keys, referred to as *Additional Master Keys x*, where x has a value between 1 and 15. It shall be an issuer option to personalise one or several of these additional sets of symmetric master keys. If the Additional Master Keys implementer-option is supported, the set of master keys to be used is identified by the 'Master Keys ID' (bits b8-b5 of byte 7) in the *Profile Control*. If the Cryptogram Version '5'-only implementer-option is supported, *Additional Master Keys x* is a set of Triple DES keys, each with a length of 16 bytes. If the Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option is supported, *Additional Master Keys x* is either a set of Triple DES keys, each with a length of 16 bytes, or a set of AES keys, each with the same length of either 16, 24 or 32 bytes.

21.11 *Additional Security Limits*

Template: -
Tag: 'E2'
Length (in bytes): var.
Format: b

Description: *Additional Security Limits* is supported when the Additional Master Keys implementer-option (see Section 15.2) and the Application Security Counters implementer-option (see Section 18) are supported.

For each additional set of symmetric master keys *Additional Master Keys x* stored in the CPACE application, this template encapsulates *Additional Security Limits x*.

If supported, this template is not retrievable from the application. The template may be updated using the PUT DATA command.

21.12 *Additional Security Limits x*

Template: 'E2'
Tag: 'DF0x'
Length (in bytes): 4
Format: b

Description: *Additional Security Limits x* is supported when the Additional Master Keys implementer-option (see Section 15.2) and the Application Security Counters implementer-option (see Section 18) are supported.

x may have any value between 1 and 15 and is coded in the second byte of the tag 'DF0x'.

Each *Additional Security Limits x* is coded as shown in Table 46.

If supported, *Additional Security Limits x* are not retrievable from the application. One or several *Additional Security Limits x* may be updated using the PUT DATA command for the template tag 'E2' and tag 'DF0x' in the command data field.

Byte	Data Element
1 - 2	*Additional AC Session Key Counter Limit x*
3 - 4	*Additional SMI Session Key Counter Limit x*

Table 46: *Additional Security Limits x* Coding

21.13 *Additional Security Limits Status*

Template: -
Tag: 'D8'
Length (in bytes): 4
Format: b

Description: *Additional Security Limits Status* is supported when the Additional Master Keys implementer-option (see Section 15.2) and the Application Security Counters implementer-option (see Section 18) are supported.

Additional Security Limits Status is coded as shown in Table 47.

The value of this data element indicates for all *Additional Master Key for AC x* and for all *Additional Master Key for SMI x* whether the limit for a security counter that limits the number of times the respective key is used has been reached.

If supported, *Additional Security Limits Status* may be retrieved from the application using the GET DATA command, but cannot be updated with the PUT DATA command.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	1	-	-	-	-	-	-	-	AC Session Key Counter Limit 1 Exceeded
	-	1	-	-	-	-	-	-	SMI Session Key Counter Limit 1 Exceeded
	-	-	1	-	-	-	-	-	AC Session Key Counter Limit 2 Exceeded
	-	-	-	1	-	-	-	-	SMI Session Key Counter Limit 2 Exceeded
	-	-	-	-	1	-	-	-	AC Session Key Counter Limit 3 Exceeded
	-	-	-	-	-	1	-	-	SMI Session Key Counter Limit 3 Exceeded
	-	-	-	-	-	-	1	-	AC Session Key Counter Limit 4 Exceeded
	-	-	-	-	-	-	-	1	SMI Session Key Counter Limit 4 Exceeded
2	1	-	-	-	-	-	-	-	AC Session Key Counter Limit 5 Exceeded
	-	1	-	-	-	-	-	-	SMI Session Key Counter Limit 5 Exceeded
	-	-	1	-	-	-	-	-	AC Session Key Counter Limit 6 Exceeded
	-	-	-	1	-	-	-	-	SMI Session Key Counter Limit 6 Exceeded
	-	-	-	-	1	-	-	-	AC Session Key Counter Limit 7 Exceeded
	-	-	-	-	-	1	-	-	SMI Session Key Counter Limit 7 Exceeded
	-	-	-	-	-	-	1	-	AC Session Key Counter Limit 8 Exceeded
	-	-	-	-	-	-	-	1	SMI Session Key Counter Limit 8 Exceeded

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
3	1	-	-	-	-	-	-	-	AC Session Key Counter Limit 9 Exceeded
	-	1	-	-	-	-	-	-	SMI Session Key Counter Limit 9 Exceeded
	-	-	1	-	-	-	-	-	AC Session Key Counter Limit 10 Exceeded
	-	-	-	1	-	-	-	-	SMI Session Key Counter Limit 10 Exceeded
	-	-	-	-	1	-	-	-	AC Session Key Counter Limit 11 Exceeded
	-	-	-	-	-	1	-	-	SMI Session Key Counter Limit 11 Exceeded
	-	-	-	-	-	-	1	-	AC Session Key Counter Limit 12 Exceeded
	-	-	-	-	-	-	-	1	SMI Session Key Counter Limit 12 Exceeded
4	1	-	-	-	-	-	-	-	AC Session Key Counter Limit 13 Exceeded
	-	1	-	-	-	-	-	-	SMI Session Key Counter Limit 13 Exceeded
	-	-	1	-	-	-	-	-	AC Session Key Counter Limit 14 Exceeded
	-	-	-	1	-	-	-	-	SMI Session Key Counter Limit 14 Exceeded
	-	-	-	-	1	-	-	-	AC Session Key Counter Limit 15 Exceeded
	-	-	-	-	-	1	-	-	SMI Session Key Counter Limit 15 Exceeded
	-	-	-	-	-	-	x	x	RFU

Table 47: *Additional Security Limits Status* Coding

21.14 *Additional SMI Session Key Counter x*

Template: -
Tag: -
Length (in bytes): 2
Format: b

Description: *Additional SMI Session Key Counter x* is supported when the Additional Master Keys implementer-option (see Section 15.2) and the Application Security Counters implementer-option (see Section 18) are supported.

x may have a value between 1 and 15 and indicates *Additional Master Key for SMI x*, to which *Additional SMI Session Key Counter x* is assigned.

Additional SMI Session Key Counter x is the internal counter defined by this specification that counts the number of Secure Messaging for Integrity session key derivations using *Additional Master Key for SMI x* that are not followed by successful validation of a Secure Messaging MAC, over the lifetime of the CPACE application.

21.15 *Additional SMI Session Key Counter Limit x*

Template: -
Tag: -
Length (in bytes): 2
Format: b

Description: *Additional SMI Session Key Counter Limit x* is supported when the Additional Master Keys implementer-option (see Section 15.2) and the Application Security Counters implementer-option (see Section 18) are supported.

x may have a value between 1 and 15 and indicates *Additional Master Key for SMI x*, to which *Additional SMI Session Key Counter Limit x* is assigned.

Additional SMI Session Key Counter Limit x is the limit defined by this specification that limits the number of Secure Messaging for Integrity session key derivations using *Additional Master Key for SMI x* that are not followed by successful validation of a Secure Messaging MAC, over the lifetime of the CPACE application.

21.16 *AID*

Template: -
Tag: '4F'
Length (in bytes): 5-16
Format: b

Description: The *AID* assigned to the CPACE application, with which the CPACE application is currently selected.

Though a tag is defined for the *AID*, it cannot be obtained from the application using the GET DATA command and cannot be updated using the PUT DATA command.

21.17 *AID-Interface Entry*

Template: -
Tag: -
Length (in bytes): var.
Format: b

Description: Each record of the AID-Interface File contains an *AID-Interface Entry*.

An *AID-Interface Entry* is the concatenation of the TLV coded data objects listed in Table 48.

An *AID-Interface Entry* may contain filler bytes '00' at its end.

The mandatory data objects shall be present in the *AID-Interface Entry* in the sequence indicated in Table 48. If the *GPO Parameters Reference Template* is present, then it shall be the last data object in the *AID-Interface Entry*.

The *Interface Descriptor* immediately contained in the *AID-Interface Entry* (i.e. the second data object in the *AID-Interface Entry*) indicates to which interface(s) the *AID-Interface Entry* applies.

The *DF-Name* contained in the *AID-Interface Entry* must be identical with (one of) the AID(s) assigned to the CPACE application.

The same *DF Name* may be contained in two *AID-Interface Entries* but only if the *Interface Descriptor*s in these *AID-Interface Entries* have different values, i.e. if the two *AID-Interface Entries* containing the same *DF Name* apply to different interfaces.

With the exception of this duplication of *DF Name*s, the *DF Name*s in the *AID-Interface Entries* must be different. In addition, the following rule in Section 12.3.1 of [EMV 1] applies to *DF Name*s in the *AID-Interface Entries* which begin with the same sub-AID:

- All *DF Name*s beginning with the same sub-*DF Name* must be distinguished by adding unique data to this common sub-*DF Name*.
- All *DF Name*s beginning with the same sub-*DF Name* must be longer than this common sub-*DF Name*.

This rule must be observed by the issuer of the CPACE application. Correct processing of the CPACE application relies on adherence to this rule. But the CPACE application does not check whether it has been observed by the issuer.

If the *GPO Parameters Reference Template* is absent from the *AID-Interface Entry*, then the default value '01' shall be used as *GPO Parameters Reference* for all interface(s) to which the *AID-Interface Entry* applies.

If the *GPO Parameters Reference Template* is present in the *AID-Interface Entry*, then its value field shall contain the data objects listed in Table 49 according to one of the following cases a), b) or c):

a) The *GPO Parameters Reference Template* contains only one data object, the *GPO Parameters Reference*.

b) The *GPO Parameters Reference Template* contains one pair of data objects, consisting of an *Interface Descriptor* followed by a *GPO Parameters Reference*. The *Interface Descriptor* shall indicate only one interface.

c) The *GPO Parameters Reference Template* contains two consecutive pairs of data objects, each consisting of an *Interface*

Descriptor followed by a *GPO Parameters Reference*. The *Interface Descriptor*s in the two pairs shall indicate different interfaces.

Case a) indicates, that the *GPO Parameters Reference* contained in the *GPO Parameters Reference Template* shall be used for all interface(s) to which the *AID-Interface Entry* applies.

Cases b) and c) are only allowed, if the *AID-Interface Entry* applies to both interfaces.

Case b) indicates, that the *GPO Parameters Reference* contained in the *GPO Parameters Reference Template* shall only be used for the interface indicated by the *Interface Descriptor* contained in the *GPO Parameters Reference Template*. The default value '01' shall be used as *GPO Parameters Reference* for the other interface.

Case c) indicates, that the *GPO Parameters Reference*s contained in the *GPO Parameters Reference Template* shall be used for the interface indicated by the *Interface Descriptor*s contained in the *GPO Parameters Reference Template* and immediately preceding the *GPO Parameters Reference*.

Tag	Length (in bytes)	Format	Value	Presence
'84'	1-16	b	*DF Name* (AID)	M
'91'	1	b	*Interface Descriptor* (see Table 50)	M
'A5'	var.	b	*FCI Proprietary Template*	M
'E1'	var.	b	*GPO Parameters Reference Template* (see Table 49)	O

Table 48: Data Objects in the *AID-Interface Entry*

Tag	Length (in bytes)	Format	Value	Presence
'91'	1	b	*Interface Descriptor* (see Table 50)	O
'C1'	1	b	*GPO Parameters Reference*, binary value in the range from '01' to '7F'	M

Table 49: Data Objects in the *GPO Parameters Reference Template*

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x	-	-	RFU
						x	x	Applicable to
						1	1	CONTACT AND CONTACTLESS
						1	0	CONTACTLESS
-	-	-	-	-	-	0	1	CONTACT
-	-	-	-	-	-	0	0	N/A

Table 50: *Interface Descriptor* Coding

21.18 *AID-Interface File Entry*

Template: -
Tag: 'D6'
Length (in bytes): 2
Format: b

Description: Devices that read the AID-Interface File from a CPACE application use the *AID-Interface File Entry* to determine the location (SFI) and the maximum number of records to be read (that is, the maximum number of *AID-Interface Entries*) in the file. The actual number of *AID-Interface Entries* in the AID-Interface File may be less than the maximum number indicated in the *AID-Interface File Entry*.

The *AID-Interface File Entry* is coded as shown in Table 51.

The *AID-Interface File Entry* may be obtained from the application using the GET DATA command, but cannot be updated using the PUT DATA command.

Note:

Coding of the *AID-Interface File Entry* has to be consistent with the actual parameters of the AID-Interface File the in which the *AID-Interface Entries* are stored. Changing the *AID-Interface File Entry* does not change the location and size of the AID-Interface File.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	-	-	-	SFI of the AID-Interface File
	-	-	-	-	-	x	x	x	RFU
2	x	x	x	x	x	x	x	x	Maximum number of *AID-Interface Entries* in the AID-Interface File

Table 51: *AID-Interface File Entry* Coding

21.19 *AIP/AFL Entry x*

Template: 'BF41'
Tag: 'DF0x'
Length (in bytes): var. (3+n*4)
Format: b

Description: *AIP/AFL Entry x* indicates the issuer's choice of AIP and AFL used in Initiate Application Processing to generate the response to the GET PROCESSING OPTIONS command for all profiles using this *AIP/AFL Entry x*.

x may have any value between 1 and 15 and is coded in the second byte of the tag 'DF0X'.

The *AIP/AFL Entry x* used for the transaction is identified in the Profile Control y for the transaction. If the AIP/AFL Entry ID in the Profile Control = x, then *AIP/AFL Entry x* will be used for the transaction.

AIP/AFL Entry x is coded as shown in Table 52.

Position	Data	Length (in bytes)	Format	Value
Bytes 1 - 2	*AIP x*	2	b	*Application Interchange Profile (AIP)* indicates the capabilities of the card to support specific functions in the application as defined in [EMV 3]. In addition to the definition in [EMV 3], bit b1 of byte 2 that has been reserved for use by contactless specifications indicates whether the application supports the Relay Resistance Protocol. *Application Interchange Profile (AIP)* is coded as shown in Table 53.
Byte 3	AFL x Length L	1	b	The length of the *AFL* is a multiple of 4
Bytes 4 - 3+L	*AFL x*	L	b	*Application File Locator (AFL)* indicates the location (SFI, range of records) of the AEFs related to a given application as defined in [EMV 3].

Table 52: *AIP/AFL Entry x* Coding

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	-	-	-	-	-	-	-	RFU
	-	1	-	-	-	-	-	-	SDA Supported
	-	-	1	-	-	-	-	-	DDA supported
	-	-	-	1	-	-	-	-	Cardholder verification is supported
	-	-	-	-	1	-	-	-	Terminal risk management is to be performed
	-	-	-	-	-	1	-	-	Issuer Authentication is supported
	-	-	-	-	-	-	x	-	RFU
	-	-	-	-	-	-	-	1	CDA supported
2	1	-	-	-	-	-	-	-	EMV mode is supported[5)]
	-	x	x	x	x	x	x	-	RFU
	-	-	-	-	-	-	-	1	Relay Resistance Protocol is supported[6)]

Table 53: *Application Interchange Profile (AIP)* Coding

21.20 *Application Control*

Template: -
Tag: 'C1'
Length (in bytes): 4
Format: b

Description: *Application Control* activates or de-activates functions of the CPACE application according to [CPA].

Bits b4 through b1 of byte 4 are defined by this specification.

Application Control is coded as shown in Table 54.

5) EMV mode is the only mode supported by CPACE for contactless transaction processing. Therefore this bit must be set to 1b in the *AIP* if the respective *AIP/AFL Entry x* is used in a profile which is applicable for contactless transaction processing.

6) This bit may only be set to 1b if the Relay Resistance Protocol implementer-option is supported. This bit must be set to 1b in the *AIP* if the respective *AIP/AFL Entry x* is used in a profile which supports the Relay Resistance Protocol for contactless transaction processing according to the value of the 'Relay Resistance Protocol Supported' bit (byte 3, bit b8) in the Proprietary Issuer Options Profile Parameters part of the *Issuer Options Profile Control x*.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	1	-	-	-	-	-	-	-	Issuer Authentication Required to be performed
	-	1	-	-	-	-	-	-	Issuer Authentication Required to Pass when Performed
	-	-	1	-	-	-	-	-	Issuer Authentication Requirements apply to Resetting of Non-Velocity-Checking Indicators and Counters[7)]
	-	-	-	1	-	-	-	-	Issuer Authentication Requirements apply to Resetting of Velocity-Checking Counters[8)]
	-	-	-	-	x	-	-	-	Key pair used for Offline Enciphered PIN Verification[9)]
	-	-	-	-	0	-	-	-	Use ICC Public/Private key pair
	-	-	-	-	1	-	-	-	Use ICC PIN Encipherment Public/Private key pair
	-	-	-	-	-	1	-	-	Offline Enciphered PIN Verification Supported
	-	-	-	-	-	-	1	-	Offline Plaintext PIN Verification Supported
	-	-	-	-	-	-	-	1	Allow Retrieval of Values and Limits of Accumulators and Counters
2	x	-	-	-	-	-	-	-	Use Default Update Counters to Control Offline Counters if CSU is Generated by Issuer Proxy
	0	-	-	-	-	-	-	-	Use Update Counters Received in CSU to Control Offline Counters if CSU is Generated by Issuer Proxy
	1	-	-	-	-	-	-	-	Use Default Update Counters in Application Control to Control Offline Counters if CSU is Generated by Issuer Proxy
	-	x	x	-	-	-	-	-	Default Update Counters
	-	0	0	-	-	-	-	-	Do Not Update Offline Counters
	-	0	1	-	-	-	-	-	Set Offline Counters to Upper Offline Limits
	-	1	0	-	-	-	-	-	Reset Offline Counters to Zero
	-	1	1	-	-	-	-	-	Add Transaction to Offline Counters
	-	-	-	x	-	-	-	-	RFU
	-	-	-	-	1	-	-	-	Activate Profile Selection File
	-	-	-	-	-	1	-	-	Amounts Included in CDOL2
	-	-	-	-	-	-	x	x	RFU
3	1	-	-	-	-	-	-	-	Log Declined Transactions
	-	1	-	-	-	-	-	-	Log Approved Transactions
	-	-	x	-	-	-	-	-	Log Offline Only
	-	-	1	-	-	-	-	-	Log Offline Only
	-	-	0	-	-	-	-	-	Log Both Offline and Online
	-	-	-	1	-	-	-	-	Log the ATC
	-	-	-	-	1	-	-	-	Log the CID
	-	-	-	-	-	1	-	-	Log the CVR
	-	-	-	-	-	-	1	-	Log the Profile ID
	-	-	-	-	-	-	-	x	RFU

7) If Issuer Authentication is required to be performed, Issuer Authentication is mandatory for resetting of non-velocity-checking indicators and counters.

8) If Issuer Authentication is required to be performed, Issuer Authentication is mandatory for resetting of velocity-checking indicators and counters.

9) Only if a separate ICC PIN Encipherment Public/Private key pair is available, this bit is evaluated by the VERIFY command.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
4	x	-	-	-	-	-	-	-	RFU
	-	x	x	x	x	x	x	x	**Used by CPACE**
	-	x	x	-	-	-	-	-	**Reserved for CPACE-SE**
	-	-	-	1	-	-	-	-	**Log Online Requests**
	-	-	-	-	x	-	-	-	**RFU**
	-	-	-	-	-	1	-	-	**Use Additional Accumulator and Counter**
	-	-	-	-	-	-	1	-	**Allow Profile Selection with Extended Check Types**
	-	-	-	-	-	-	-	1	**Allow Extended Controls**

Table 54: *Application Control* Coding

21.21 *Application Decisional Results (ADR)*

Template: -
Tag: -
Length (in bytes): 6
Format: b

Description: The data element *Application Decisional Results (ADR)* is used internal to the application to indicate exception conditions that occurred during the current and previous transactions. The Card Issuer Action Codes (CIAC - Decline, CIAC - Default, and CIAC - Online) are each compared to the *Application Decisional Results (ADR)* to determine whether the transaction shall be declined offline or go online. The format and coding of *Application Decisional Results (ADR)* is the same as for each CIAC, described in Table 56.

21.22 *Card Issuer Actions Codes Entry x (CIACs Entry x)*

Template: 'BF34'
Tag: 'DF0x'
Length (in bytes): 18
Format: b

Description: A *Card Issuer Actions Codes Entry x (CIACs Entry x)* consists of the concatenation of the CIACs for Decline, Default, and Online. Each CIAC is compared to the *Application Decisional Results (ADR)* to take transaction decisions for all Profiles using this *Card Issuer Actions Codes Entry x (CIACs Entry x)*.

x may have any value between 1 and 15 and is coded in the second byte of the tag 'DF0x'.

CIAC - Decline: Used by the issuer to set the situations when a transaction is always declined at the first or second GENERATE AC.

CIAC - Default: Used by the issuer to set the situations when a transaction is declined if the terminal is not online-capable or if connection to the issuer is not possible.

CIAC - Online: Used by the issuer to set the situations when a transaction goes online if the terminal is online-capable.

A *Card Issuer Actions Codes Entry x (CIACs Entry x)* is coded as shown in Table 55.

Position	Data	Length
Bytes 1 - 6	CIAC - Decline	6 bytes
Bytes 7 - 12	CIAC - Default	6 bytes
Bytes 13 - 18	CIAC - Online	6 bytes

Table 55: *Card Issuer Actions Codes Entry x (CIACs Entry x)*

Each CIAC is coded as shown in Table 56.

'Accumulator 3 Lower Limit Exceeded' (byte 3, bit b3), 'Accumulator 3 Upper Limit Exceeded' (byte 4, bit b3), 'Counter 4 Lower Limit Exceeded' (byte 3, bit b2), 'Counter 4 Upper Limit Exceeded' (byte 4, bit b2) are used by this specification in accordance with section 19.3.1 of [CPA]. These bits are only relevant, if the 'Use Additional Accumulators and Counter' bit (byte 4, bit b3) in the *Application Control* of a CPACE application has the value 1b.

The 'Transaction with Cashback' bit (byte 6, bit b8) and the 'RRP without CDA' bit (byte 6, bit b7) are defined by this specification.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	1	-	-	-	-	-	-	-	Last Online Transaction Not Completed
	-	1	-	-	-	-	-	-	Go Online On Next Transaction Was Set
	-	-	1	-	-	-	-	-	Issuer Script Processing Failed
	-	-	-	1	-	-	-	-	Issuer Authentication Failed
	-	-	-	-	1	-	-	-	Issuer Authentication Data Not Received in Online Response
	-	-	-	-	-	1	-	-	PIN Try Limit Exceeded
	-	-	-	-	-	-	1	-	Offline PIN Verification Not Performed
	-	-	-	-	-	-	-	1	Offline PIN Verification Failed
2	1	-	-	-	-	-	-	-	Unable To Go Online
	-	1	-	-	-	-	-	-	Terminal Erroneously Considers Offline PIN OK
	-	-	1	-	-	-	-	-	Script Received
	-	-	-	1	-	-	-	-	Offline Data Authentication Failed on Previous Transaction
	-	-	-	-	1	-	-	-	Match Found In Additional Check Table 1
	-	-	-	-	-	1	-	-	No Match Found In Additional Check Table 1
	-	-	-	-	-	-	1	-	Match Found In Additional Check Table 2
	-	-	-	-	-	-	-	1	No Match Found In Additional Check Table 2
3	1	-	-	-	-	-	-	-	Accumulator 1 Lower Limit Exceeded
	-	1	-	-	-	-	-	-	Accumulator 2 Lower Limit Exceeded
	-	-	1	-	-	-	-	-	Counter 1 Lower Limit Exceeded
	-	-	-	1	-	-	-	-	Counter 2 Lower Limit Exceeded
	-	-	-	-	1	-	-	-	Counter 3 Lower Limit Exceeded
	-	-	-	-	-	1	-	-	**Accumulator 3 Lower Limit Exceeded**
	-	-	-	-	-	-	1	-	**Counter 4 Lower Limit Exceeded**
	-	-	-	-	-	-	-	1	Number of Days Offline Limit Exceeded
4	1	-	-	-	-	-	-	-	Accumulator 1 Upper Limit Exceeded
	-	1	-	-	-	-	-	-	Accumulator 2 Upper Limit Exceeded
	-	-	1	-	-	-	-	-	Counter 1 Upper Limit Exceeded
	-	-	-	1	-	-	-	-	Counter 2 Upper Limit Exceeded
	-	-	-	-	1	-	-	-	Counter 3 Upper Limit Exceeded
	-	-	-	-	-	1	-	-	**Accumulator 3 Upper Limit Exceeded**
	-	-	-	-	-	-	1	-	**Counter 4 Upper Limit Exceeded**
	-	-	-	-	-	-	-	1	MTA exceeded
5	x	-	-	-	-	-	-	-	Not used
	-	x	-	-	-	-	-	-	Not used
	-	-	x	-	-	-	-	-	Not used
	-	-	-	1	-	-	-	-	Check Failed
	-	-	-	-	x	x	x	x	RFU
6	1	-	-	-	-	-	-	-	**Transaction with Cashback**
	-	1	-	-	-	-	-	-	**RRP without CDA**
	-	-	x	x	x	x	x	x	Reserved for Use by CPACE

Table 56: Card Issuer Action Code Coding

21.23 *Card Status Update (CSU)*

Template: -
Tag: -
Length (in bytes): 4
Format: b

Description: *Card Status Update (CSU)* contains data sent to the CPACE application by the issuer to indicate whether the issuer approves or declines the transaction, and to initiate actions specified by the issuer.

According to this specification, *Card Status Update (CSU)* is coded as shown in Table 57.

Bytes 1 and 2 of *Card Status Update (CSU)* are defined by [CPA]. Byte 4 is defined by this specification.

The interpretation of 'Update Counters' in byte 2 of *Card Status Update (CSU)* depends on the value of 'Individual Update of Accumulators and Counters' in byte 4 of *Card Status Update (CSU)*:

- If 'Individual Update of Accumulators and Counters' in byte 4 of *Card Status Update (CSU)* has the value 0b, then 'Update Counters' shall be interpreted as defined by [CPA].
- If 'Individual Update of Accumulators and Counters' in byte 4 of *Card Status Update (CSU)* has the value 1b, then 'Update Counters' shall be interpreted as defined by this specification (see Section 13.2.6).

According to this specification, byte 3 in the *Card Status Update (CSU)* may be used by the issuer to activate or deactivate contactless access to the CPACE card when the Contactless Control - Card implementer-option is supported or to activate or deactivate contactless access to the CPACE application when the Contactless Control - Application implementer-option is supported.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	1	-	-	-	-	-	-	-	Proprietary Authentication Data (PAD) Included
	-	x	x	x	-	-	-	-	RFU
	-	-	-	-	x	x	x	x	PIN Try Counter
2	1	-	-	-	-	-	-	-	Issuer Approves Online Transaction
	-	1	-	-	-	-	-	-	Card Block
	-	-	1	-	-	-	-	-	Application Block
	-	-	-	1	-	-	-	-	Update PIN Try Counter
	-	-	-	-	1	-	-	-	Set Go Online on Next Transaction
	-	-	-	-	-	1	-	-	CSU Created by Proxy for the Issuer
	-	-	-	-	-	-	x	x	Update Counters (**Accumulator 1**)
	-	-	-	-	-	-	0	0	Do Not Update Offline Counters (**Accumulator 1**)
	-	-	-	-	-	-	0	1	Set Offline Counters (**Accumulator 1**) to Upper Offline Limits
	-	-	-	-	-	-	1	0	Reset Offline Counters (**Accumulator 1**)to Zero
	-	-	-	-	-	-	1	1	Add Transaction to Offline Counters (**Accumulator 1**)
3	x	-	-	-	-	-	-	-	Deactivate contactless
	0	-	-	-	-	-	-	-	DO NOT DEACTIVATE
	1	-	-	-	-	-	-	-	DEACTIVATE
	-	x	-	-	-	-	-	-	Activate contactless
	-	0	-	-	-	-	-	-	DO NOT ACTIVATE
	-	1	-	-	-	-	-	-	ACTIVATE
	-	-	x	-	-	-	-	-	Apply activation/deactivation of contactless to (only applicable if b8 or b7 = 1b)
	-	-	0	-	-	-	-	-	APPLICATION
	-	-	1	-	-	-	-	-	CARD
	-	-	-	x	x	x	x	x	RFU

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
4	1	-	-	-	-	-	-	-	**Individual Update of Accumulators and Counters**
	-	1	-	-	-	-	-	-	**New Number of Days Offline Limit**
	-	-	x	x	-	-	-	-	**New Accumulator 1 Upper Limit**
	-	-	1	-	-	-	-	-	**Limit 0**
	-	-	-	1	-	-	-	-	**Limit 1**
	-	-	-	-	x	x	-	-	**Update Accumulator 2**
	-	-	-	-	0	0	-	-	**Do Not Update Accumulator 2**
	-	-	-	-	0	1	-	-	**Set Accumulator 2 to Upper Limit**
	-	-	-	-	1	0	-	-	**Reset Accumulator 2 to Zero**
	-	-	-	-	1	1	-	-	**Add Transaction to Accumulator 2**
	-	-	-	-	-	-	x	x	**Update Accumulator 3**
	-	-	-	-	-	-	0	0	**Do Not Update Accumulator 3**
	-	-	-	-	-	-	0	1	**Set Accumulator 3 to Upper Limit**
	-	-	-	-	-	-	1	0	**Reset Accumulator 3 to Zero**
	-	-	-	-	-	-	1	1	**Add Transaction to Accumulator 3**

Table 57: *Card Status Update (CSU)* Coding

21.24 *Card Verification Results (CVR)*

Template: -
Tag: '9F52'
Length (in bytes): 5
Format: b

Description: *Card Verification Results (CVR)* are used to inform the issuer about exception conditions that occurred during the current and previous transactions. It is transmitted to the terminal in the *Issuer Application Data*.

Bits b4 and b3 of byte 3 in *Card Verification Results (CVR)* are defined by this specification. All other bits are defined by [CPA].

Though a tag is defined for the *Card Verification Results (CVR)*, it is not possible to retrieve the *Card Verification Results (CVR)* with the GET DATA command or to update the *Card Verification Results (CVR)* with the PUT DATA command.

Card Verification Results (CVR) are coded as shown in Table 58.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	-	-	-	-	-	-	AC Type Returned in Second GENERATE AC
	0	0	-	-	-	-	-	-	AAC
	0	1	-	-	-	-	-	-	TC
	1	0	-	-	-	-	-	-	Second GENERATE AC Not requested
	1	1	-	-	-	-	-	-	RFU
	-	-	x	x	-	-	-	-	AC Type Returned in First GENERATE AC
	-	-	0	0	-	-	-	-	AAC
	-	-	0	1	-	-	-	-	TC
	-	-	1	0	-	-	-	-	ARQC
	-	-	1	1	-	-	-	-	RFU
	-	-	-	-	1	-	-	-	CDA performed
	-	-	-	-	-	1	-	-	Offline DDA Performed
	-	-	-	-	-	-	1	-	Issuer Authentication Not Performed
	-	-	-	-	-	-	-	1	Issuer Authentication Failed
2	x	x	x	x	-	-	-	-	Low Order Nibble of PIN Try Counter
	-	-	-	-	1	-	-	-	Offline PIN Verification Performed
	-	-	-	-	-	1	-	-	Offline PIN Verification Performed and PIN Not Successfully Verified
	-	-	-	-	-	-	1	-	PIN Try Limit Exceeded
	-	-	-	-	-	-	-	1	Last Online Transaction Not Completed
3	1	-	-	-	-	-	-	-	Lower Offline Transaction Count Limit Exceeded
	-	1	-	-	-	-	-	-	Upper Offline Transaction Count Limit Exceeded
	-	-	1	-	-	-	-	-	Lower Cumulative Offline Amount Limit Exceeded
	-	-	-	1	-	-	-	-	Upper Cumulative Offline Amount Limit Exceeded
	-	-	-	-	x	-	-	-	**Not used**
	-	-	-	-	-	1	-	-	**Terminal Erroneously considers Offline PIN OK**
	-	-	-	-	-	-	1	-	Check Failed
	-	-	-	-	-	-	-	1	Match Found in any Additional Check Table
4	x	x	x	x	-	-	-	-	Number of Issuer Script Commands Containing Secure Messaging Processed
	-	-	-	-	1	-	-	-	Issuer Script Processing Failed
	-	-	-	-	-	1	-	-	Offline Data Authentication Failed on Previous Transaction
	-	-	-	-	-	-	1	-	Go Online on Next Transaction Was Set
	-	-	-	-	-	-	-	1	Unable to Go Online
5	x	x	x	x	x	x	x	x	RFU

Table 58: *Card Verification Results (CVR)* Coding

21.25 *Contactless Command Access*

Template: 'E0'
Tag: 'DF01'
Length (in bytes): 2
Format: b

Description: *Contactless Command Access* is supported when the Contactless Command Access Controls implementer-option is supported. This data element is used to enable/disable support of commands for the application on the contactless interface.

Contactless Command Access is coded as shown in Table 59.

The *Contactless Command Access* may be obtained from the application using the GET DATA command for the template tag 'E0', and may be updated using the PUT DATA command for the template tag 'E0' and tag 'DF01' in the command data field.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	-	-	-	-	-	-	-	VERIFY command with Offline Enciphered PIN on contactless interface
	1	-	-	-	-	-	-	-	ALLOWED
	0	-	-	-	-	-	-	-	NOT ALLOWED
	-	x	-	-	-	-	-	-	INTERNAL AUTHENTICATE command on contactless interface
	-	1	-	-	-	-	-	-	ALLOWED
	-	0	-	-	-	-	-	-	NOT ALLOWED
	-	-	x	-	-	-	-	-	GET CHALLENGE command on contactless interface
	-	-	1	-	-	-	-	-	ALLOWED
	-	-	0	-	-	-	-	-	NOT ALLOWED
	-	-	x	x	x	x	x	x	RFU
2	x	x	x	x	x	x	x	x	RFU

Table 59: *Contactless Command Access* Coding

21.26 *Contactless Command Access Controls*

Template: -
Tag: 'E0'
Length (in bytes): var.
Format: b

Description: *Contactless Command Access Controls* is supported when the Contactless Command Access Controls implementer-option is supported. This template contains

- *Contactless Command Access* (tag 'DF01'),
- *Contactless READ RECORD Access* (tag 'DF02') and
- *Contactless GET DATA Access* (tag 'DF03').

This template may be obtained from the application using the GET DATA command and may be updated using the PUT DATA command.

21.27 *Contactless Control - Application*

Template: -
Tag: 'D4'
Length (in bytes): 1
Format: b

Description: *Contactless Control - Application* is supported when the Contactless Control - Application implementer-option is supported. This data element is used to:

- Control activation and deactivation of contactless access to the application,
- Indicate, whether the application has the right to activate/deactivate contactless access to the card.

Contactless Control - Application is coded as shown in Table 60.

The *Contactless Control - Application* may be obtained from the application using the GET DATA command and may be updated using the PUT DATA command.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	-	-	-	-	-	-	-	State of contactless access to the application
1	-	-	-	-	-	-	-	ACTIVATED
0	-	-	-	-	-	-	-	DEACTIVATED
-	x	x	-	-	-	-	-	Enablement of unsecured DEACTIVATE CL command for the application
-	1	1	-	-	-	-	-	ENABLED FOR CONTACT AND CONTACTLESS
-	1	0	-	-	-	-	-	ENABLED FOR CONTACT
-	0	1	-	-	-	-	-	ENABLED FOR CONTACTLESS
-	0	0	-	-	-	-	-	DISABLED
-	-	-	x	-	-	-	-	Activation of contactless access to the application with SELECT of the application on the contact interface
-	-	-	1	-	-	-	-	ENABLED
-	-	-	0	-	-	-	-	DISABLED
-	-	-	-	x	-	-	-	Activation of contactless access to the application with successful VERIFY command on the contact interface
-	-	-	-	1	-	-	-	ENABLED
-	-	-	-	0	-	-	-	DISABLED
-	-	-	-	-	x	-	-	Activation of contactless access to the application with second GENERATE AC and successful Issuer Authentication on the contact interface
-	-	-	-	-	1	-	-	ENABLED
-	-	-	-	-	0	-	-	DISABLED
-	-	-	-	-	-	x	-	Right of application to activate/deactivate contactless access to the card[10)]
-	-	-	-	-	-	1	-	ENABLED
-	-	-	-	-	-	0	-	DISABLED
							x	RFU

Table 60: *Contactless Control - Application* Coding

[10)] 'Right of application to activate/deactivate contactless access to the card' in *Contactless Control - Application* is evaluated only if the Activation/Deactivation of Contactless Access to Dual Interface Cards implementer-option is supported.

21.28 *Contactless Control - Card*

Template: -
Tag: 'D3'
Length (in bytes): 1
Format: b

Description: *Contactless Control - Card* is supported when the Contactless Control - Card implementer-option is supported for dual interface cards.

This data element is defined on card level. Only one value of this data element is defined for all CPACE applications residing on a dual interface card.

It is used to control activation and deactivation of contactless access to the card.

Contactless Control - Card is coded as shown in Table 61.

The *Contactless Control - Card* may be obtained from the application using the GET DATA command and may be updated using the PUT DATA command.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	-	-	-	-	-	-	-	State of contactless access to the card
1	-	-	-	-	-	-	-	ACTIVATED
0	-	-	-	-	-	-	-	DEACTIVATED
-	x	x	-	-	-	-	-	Enablement of unsecured DEACTIVATE CL command for the card
-	1	1	-	-	-	-	-	ENABLED FOR CONTACT AND CONTACTLESS
-	1	0	-	-	-	-	-	ENABLED FOR CONTACT
-	0	1	-	-	-	-	-	ENABLED FOR CONTACTLESS
-	0	0	-	-	-	-	-	DISABLED
-	-	-	x	-	-	-	-	Activation of contactless access to the card with SELECT of an application[11)] on the contact interface
-	-	-	1	-	-	-	-	ENABLED
-	-	-	0	-	-	-	-	DISABLED
-	-	-	-	x	-	-	-	Activation of contactless access to the card with successful VERIFY command[11)] on the contact interface
-	-	-	-	1	-	-	-	ENABLED
-	-	-	-	0	-	-	-	DISABLED

11) If 'Right of application to activate/deactivate contactless access to the card' in *Contactless Control - Application* = ENABLED for the currently selected CPACE application.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	x	-	-	Activation of contactless access to the card with second GENERATE AC and successful Issuer Authentication[11)] on the contact interface
-	-	-	-	-	1	-	-	ENABLED
-	-	-	-	-	0	-	-	DISABLED
-	-	-	-	-		x	x	RFU

Table 61: *Contactless Control - Card* Coding

21.29 *Contactless READ RECORD Access*

Template:	'E0'
Tag:	'DF02'
Length (in bytes):	var.
Format:	b

Description: *Contactless READ RECORD Access* is supported when the Contactless Command Access Controls implementer-option is supported.

This data element is used to indicate:

- Either which records are allowed to be read on the contactless interface (positive access list),
- or which records are not allowed to be read on the contactless interface (negative access list).

The *Contactless READ RECORD Access* has a length of 1 + 3*n bytes, where n >= 1.

The first byte of the *Contactless READ RECORD Access* indicates, whether it is a positive access list (first byte = '00') or a negative access list (first byte = '01').

Bytes 2 to 1 + 3*n of the *Contactless READ RECORD Access* consist of n 3-byte values (called entries of the *Contactless READ RECORD Access*) which are interpreted in the same way as the first 3 bytes of AFL entries:

- The five most significant bits of the first byte indicate an SFI. The three least significant bits of the first byte shall be set to zero.
- The second byte indicates the first (or only) record number to be read / not to be read for that SFI. The second byte shall never be set to zero.
- The third byte indicates the last record number to be read /not to be read for that SFI. Its value is either greater than or equal to the second byte.

When the third byte is greater than the second byte, all the records ranging from the record number in the second byte to and including the record number in the third byte shall be read /shall not be read for that SFI. When the third byte is equal to the second byte, only the record number coded in the second byte shall be read /shall not be read for that SFI.

The *Contactless READ RECORD Access* may be obtained from the application using the GET DATA command for the template tag 'E0', and may be updated using the PUT DATA command for the template tag 'E0' and tag 'DF02' in the command data field.

21.30 *Contactless GET DATA Access*

Template:	'E0'
Tag:	'DF03'
Length (in bytes):	var.
Format:	b

Description: *Contactless GET DATA Access* is supported when the Contactless Command Access Controls implementer-option is supported.

This data element is used to indicate:

- Either which data objects are allowed to be read on the contactless interface (positive access list),
- or which data objects are not allowed to be read on the contactless interface (negative access list).

The *Contactless GET DATA Access* has a length of 1 + 2*n bytes, where n >= 1.

The first byte of the *Contactless GET DATA Access* indicates, whether it is a positive access list (first byte = '00') or a negative access list (first byte = '01').

Bytes 2 to 1 + 2*n of the *Contactless GET DATA Access* consist of n 2-byte values (called entries of the *Contactless GET DATA Access*) which are interpreted as tags in the same way as P1 | P2 of the GET DATA command.

The tags listed in bytes 2 to 1 + 2*n of the *Contactless GET DATA Access* are the tags of the data objects which are allowed /not allowed to be read on the contactless interface.

The *Contactless GET DATA Access* may be obtained from the application using the GET DATA command for the template tag 'E0', and may be updated using the PUT DATA command for the template tag 'E0' and tag 'DF03' in the command data field.

21.31 *Counter Profile Control x*

Template: 'BF36'
Tag: 'DF0x'
Length (in bytes): 1 **or 2**
Format: b

Description: *Counter Profile Control x* indicates the issuer's choice of data and behaviour to configure a Counter (1-4) within a Profile.

x may have any value between 1 and 14 and is coded in the second byte of the tag 'DF0x'.

Byte 1 of *Counter Profile Control x* is defined by [CPA]. Byte 2 is defined by this specification.

If 'Allow Extended Controls' (byte 4, bit b1) in the *Application Control* of a CPACE application has the value 0b, every *Counter Profile Control x* of the application shall have a length of 1 byte.

If 'Allow Extended Controls' in the *Application Control* of a CPACE application has the value 1b, every *Counter Profile Control x* of the application shall have a length of 1 or 2 bytes.

Counter Profile Control x is coded as shown in Table 62.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	-	-	-	-	-	RFU
	-	-	-	x	-	-	-	-	Limit Set ID
	-	-	-	0	-	-	-	-	Use Limit Set 0
	-	-	-	1	-	-	-	-	Use Limit Set 1
	-	-	-	-	x	-	-	-	Allow Counting
	-	-	-	-	0	-	-	-	Do not allow Counting[12)]
	-	-	-	-	1	-	-	-	Allow Counting
	-	-	-	-	-	1	-	-	Reset Counter with Online Response
	-	-	-	-	-	-	1	-	Send Counter in IAD
	-	-	-	-	-	-	-	x	RFU
2	x	x	x	x	x	x	x	-	RFU
	-	-	-	-	-	-	-	1	Reset Counter with Offline PIN Verification

Table 62: *Counter Profile Control x* Coding

12) This setting allows Velocity Checking for Counter x to include counters that cannot be incremented in the profile selected for the transaction.

21.32 *Counter x Control*

Template:	'BF37'
Tag:	'DF0x'
Length (in bytes):	1 **or 2**
Format:	b

Description: *Counter x Control* indicates the issuer's choice of data and behaviour to configure Counter x independently of a Profile.

x may have a value between 1 and 4 and is coded in the second byte of the tag 'DF0x'.

Byte 1 of *Counter x Control* is defined by [CPA]. Byte 2 is defined by this specification.

If 'Allow Extended Controls' (byte 4, bit b1) in the *Application Control* of a CPACE application has the value 0b, every *Counter x Control* of the application shall have a length of 1 byte.

If 'Allow Extended Controls' in the *Application Control* of a CPACE application has the value 1b, every *Counter x Control* of the application shall have a length of 1 or 2 bytes.

Counter x Control is coded as shown in Table 63.

A bit in the 'Include Based on Transaction CVM' bits (byte 4, bits b4-b1) in *Counter x Control* shall be set to the value 0b if and only if the transaction is to be counted when the Cardholder Verification Method (CVM) indicated by this bit is the *Transaction CVM*.

Note:

- The value 0000b of the 'Include Based on Transaction CVM' bits indicates that accumulation shall be performed irrespective of the *Transaction CVM*, that is, irrespective of whether and how cardholder verification was performed during the current transaction.
- The determination of the *Transaction CVM* is described in Section 12.2.3.2.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	1	-	-	-	-	-	-	-	Include ARQC Transaction in CRM Test[13)]
	-	1	-	-	-	-	-	-	Include Offline Declines
	-	-	1	-	-	-	-	-	Include Offline Approvals
	-	-	-	x	-	-	-	-	Include only if not Accumulated (Transaction is not Accumulated in any non-cyclic Accumulator)[14)]
	-	-	-	0	-	-	-	-	include always
	-	-	-	1	-	-	-	-	include only if not Accumulated
	-	-	-	-	x	-	-	-	Include only if International (Terminal Country Code does not match the Issuer Country Code)[14)]
	-	-	-	-	0	-	-	-	include always
	-	-	-	-	1	-	-	-	include only if International
	-	-	-	-	-	x	x	x	RFU
2	1	-	-	-	-	-	-	-	Include Online Requests
	-	x	x	x	-	-	-	-	RFU
	-	-	-	-	x	x	x	x	Include Based on Transaction CVM
	-	-	-	-	0	-	-	-	Include if Transaction CVM is Offline PIN[14)]
	-	-	-	-	-	0	-	-	Include if Transaction CVM is Online PIN[14)]
	-	-	-	-	-	-	0	-	Include if Transaction CVM is Signature[14)]
	-	-	-	-	-	-	-	0	Include if Transaction CVM is No CVM[14)]

Table 63: *Counter x Control* Coding

13) This bit applies only if the "Include Offline Approvals" bit is set to 1b.

14) This bit does not apply to counting Offline Declines (if the "Include Offline Declines" bit is set to 1b).

21.33 *Device Estimated Transmission Time For Relay Resistance R-APDU*

Template: -
Tag: -
Length (in bytes): 2
Format: b

Description: This data element is only supported if the Relay Resistance Protocol implementer-option is supported.

Device Estimated Transmission Time For Relay Resistance R-APDU is a 2-byte binary value in units of hundreds of microseconds that represents the time taken to send the EXCHANGE RELAY RESISTANCE DATA response message.

Device Estimated Transmission Time For Relay Resistance R-APDU is stored in bytes 5 to 6 of a *RRP Configuration Data Set*.

During Relay Resistance Protocol Preparation (see Section 7.2.5), *Device Estimated Transmission Time For Relay Resistance R-APDU* is retrieved from the *RRP Configuration Data Set* and stored transiently in bytes 13 to 14 of the *RRP Transaction Data Set* for inclusion in the EXCHANGE RELAY RESISTANCE DATA response message (see Section 8.2.4) and for inclusion in the generation of the dynamic signature (see Req C.99 in Section 12.2.7.4).

21.34 *Device Relay Resistance Entropy*

Template: -
Tag: -
Length (in bytes): 4
Format: b

Description: This data element is only supported if the Relay Resistance Protocol implementer-option is supported.

Device Relay Resistance Entropy is a 4-byte random number returned in the response to the EXCHANGE RELAY RESISTANCE DATA command. It is constructed by selecting 4 bytes of the *RRP Dynamic Number*.

During EXCHANGE RELAY RESISTANCE DATA Command Processing (see Section 8.2.3), the *Device Relay Resistance Entropy* is stored transiently in bytes 5 to 8 of the *RRP Transaction Data Set* for inclusion in the generation of the dynamic signature (see Req C.99 in Section 12.2.7.4).

21.35 *Dynamic Issuer Data*

Template: -
Tag: 'D1'
Length (in bytes): var.
Format: b

Description: Issuer specific dynamic data. The value of the *Dynamic Issuer Data* will be included in the Issuer Discretionary Data of the *Issuer Application Data*, if 'Include Dynamic Issuer Data in IAD' (byte 7, bit b6) has the value 1b in the *Issuer Options Profile Control x* used for the transaction.

Dynamic Issuer Data may be obtained from the application using the GET DATA command and may be updated using the PUT DATA command.

21.36 *Environment in Use*

Template: -
Tag: 'D5'
Length (in bytes): 1
Format: b

Description: *Environment in Use* is supported when the Internal Data Logging implementer-option is supported. This data element is used by the CPACE application to store transiently the characteristics of the environment a transaction is processed in.

Environment in Use is an internal parameter of the CPACE application which cannot be obtained from the application using the GET DATA command, and cannot be updated using the PUT DATA command.

Environment in Use may be logged using the *ILDOL* (see Section 17).

Environment in Use is coded as shown in Table 64.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
-	-	-	-	-	-	-	x	Interface
-	-	-	-	-	-	-	0	CONTACT
-	-	-	-	-	-	-	1	CONTACTLESS
x	x	x	x	x	x	x	-	RFU

Table 64: *Environment in Use* Coding

21.37 *GPO Parameters x*

Template: 'BF3E'
Tag: 'DF01' - 'DF7F'
Length (in bytes): 2
Format: b

Description: *GPO Parameters x* contains the parameters used during the processing of the GET PROCESSING OPTIONS command.

x may have any value between 1 and 127 and is coded in the second byte of the tag 'DFxx'[15]. The value of x, i.e. of the second byte 'xx' of the tag 'DFxx', is the value of the *GPO Parameters Reference* which has been retrieved during Application Selection (see Req C.34).

GPO Parameters x is coded as shown in Table 65.

Byte	Data Element	Description
1	GPO Input Data Length	The value expected for the length of the GPO Input Data (the value field of the template in PDOL Related Data). The tags and lengths of these data elements were sent to the Terminal in the PDOL. The value of GPO Input Data Length must be consistent with the contents personalised in the PDOL.
2	Profile Selection Diversifier	An identifier of card data used to support profile selection based on card data. For the CPACE application this identifier is associated with the application by means of the *GPO Parameters Reference* which has been retrieved during Application Selection (see Req C.34).

Table 65: *GPO Parameters x* Coding

[15] According to [CPA], only 15 *GPO Parameters x*, identified by the tags 'DF01' to 'DF0F' shall be supported. According to this specification additional *GPO Parameters x*, identified by the tags 'DF10' to 'DF7E', shall be supported.

21.38 *Internal Flags*

Template:	-
Tag:	-
Length (in bytes):	var.
Format:	b

Description: Optional flags that may be implemented for use internal to the application.

Note:

This is an implementer-optional data element that could be used to implement the requirements for the application.

In addition to the *Internal Flags* defined in [CPA], the

'RRP Initialised' flag and the

'RRP Fatal Error' flag

are defined by this specification:

Like all Internal Flags, the 'RRP Initialised' flag and the 'RRP Fatal Error' flag shall be reset by the GET PROCESSING OPTIONS command according to Req C.44.

The 'RRP Initialised' flag shall be set, if Relay Resistance Protocol Preparation described in Section 7.2.5 has been performed successfully.

The 'RRP Fatal Error' flag shall be set, if the RRP Check described in Section 12.2.3.4 detects a kernel error regarding Relay Resistance Protocol processing which requires a decline of the transaction.

21.39 *Internal Log Data Object List (ILDOL)*

Template:	'BF40'
Tag:	'DF05'
Length (in bytes):	var.
Format:	b

Description: The *Internal Log Data Object List (ILDOL)* is supported when the Internal Data Logging implementer-option is supported.

If the Internal Data Logging implementer-option is supported, the data object containing the *ILDOL* (tag 'DF05') may be included in the *Log Data Tables* template at the issuer's discretion.

The *ILDOL* is a Data Object List (DOL), i.e. list of tags and lengths of data elements.

If the *ILDOL* is present in the *Log Data Tables* template, the list of data elements identified by the *ILDOL*

- shall be built according to the rules specified in Section 5.4 of

[EMV 3] and

- shall be included as additional card data in the transaction log record.

If the *ILDOL* is present in the *Log Data Tables* template, additional card data shall be logged for all transactions that are to be logged, regardless of whether the transaction is logged during processing of the first or second GENERATE AC command.

According to Section 5.4 of [EMV 3], in order to build the list of data elements using to the *ILDOL*, the tags in the *ILDOL* have to be "known" to the CPACE application, i.e. the CPACE application must be able to provide the current values of the respective data elements.

According to this specification, at a minimum, the CPACE shall be able to provide the current values of the data objects listed in Table 66 if the respective tags are included in the *ILDOL*, irrespective of their sequence in the *ILDOL*. If the tag of *IATD* or *ARC* is included in the *ILDOL*, the CPACE application must fill the part of the list representing the respective data object with hexadecimal zeroes.

Tags not listed in Table 66 but present in the *ILDOL* may still be treated as known by the CPACE application. But this is not required by this specification.

The *ILDOL* may be obtained from the application using the GET DATA command for template tag 'BF40', and may be updated in the application using the PUT DATA command for the template tag 'BF40' and tag 'DF05' in the command data field.

Note:

- Tags of data elements which can be retrieved from the first or second GENERATE AC command data field using the Log Data Tables defined by [CPA] are not listed in Table 66, but may be known to the CPACE application.
- The tags of *ATC*, *CID*, *CVR* and *Profile ID*, which must be known to the CPACE application, are not listed in Table 66, since logging of these data elements can be controlled using the *Application Control*.
- Using tags with less than its fixed or maximum length in the *ILDOL* is allowed according to Section 5.4 of [EMV 3]. In this way, it is possible to log only the first part of a data element.
- It has to be kept in mind, that the *ILDOL* has to be consistent with the *Log Format*.

Tag	Length (in bytes)	Format	Value
'9F26'	8	b	*Application Cryptogram*
'8A'	2	an 2	*Authorisation Response Code (ARC)*
'84'	5-16	b	*DF Name* returned in the response to the SELECT command
'D5'	1	b	*Environment in Use*, if supported by the application
'9F10'	32	b	*Issuer Application Data*
'91'	8-16	b	*Issuer Authentication Data*
'9F50'	6	n 12	*Offline Balance*
'C9'	2	n 3	*Offline Balance Currency Code*
'C7'	1	b	*Previous Transaction History (PTH)*
'C4'	1	b	*Security Limits Status*, if supported by the application

Table 66: Data Objects to be Known for *ILDOL* Processing

21.40 *Issuer Authentication Data (IATD)*

Template: -
Tag: '91'
Length (in bytes): 8-16
Format: b

Description: *Issuer Authentication Data (IATD)* are sent from the issuer or its proxy to the CPACE application for online Issuer Authentication.

The *Issuer Authentication Data (IATD)* expected by the CPACE application consists of the data elements listed in Table 67, in the order shown.

Proprietary Authentication Data (PAD) shall be present in the *Issuer Authentication Data (IATD)*, i.e. *Issuer Authentication Data (IATD)* shall have a length of 16 bytes, if and only if **all** of the following are true:

- 'Proprietary Authentication Data in IATD Supported' in the *Issuer Options Profile Control* has the value 1b,
- **and** 'Proprietary Authentication Data (PAD) Included' in *Card Status Update (CSU)* has the value 1b,
- **and** at least one of bits b8-b5 in byte 4 of *Card Status Update (CSU)* has the value 1b.

Though a tag is defined for the *Issuer Authentication Data (IATD)*, it cannot be obtained from the application using the GET DATA command and cannot be updated using the PUT DATA command.

Position	Data Element	Length (in bytes)	Format	Presence
Bytes 1 - 4	*Authorisation Response Cryptogram (ARPC)*	4	b	M
Bytes 5 - 8	*Card Status Update (CSU)*	4	b	M
Bytes 9 - 16	*Proprietary Authentication Data (PAD)*	8	b	C

Table 67: *Issuer Authentication Data (IATD)*

21.41 *Issuer Options Profile Control*

Template: -
Tag: -
Length (in bytes): 10
Format: b

Description: *Issuer Options Profile Control* is the *Issuer Options Profile Control x* used in processing the transaction according to Req C.47 in Section 12.2.1 of this document.

21.42 *Issuer Options Profile Control x*

Template:	'BF3B'
Tag:	'DF0x'
Length (in bytes):	7 **or 10**
Format:	b

Description: *Issuer Options Profile Control x* indicates the issuer options that control Card Risk Management and application behaviour within all Profiles using this *Issuer Options Profile Control x*. x may have any value between 1 and 15 and is coded in the second byte of the tag 'DF0x'.

Bytes 1 to 6 of *Issuer Options Profile Control x* are defined by [CPA]. Bytes 7 to 10 are defined by this specification.

If 'Allow Extended Controls' (byte 4, bit b1) in the *Application Control* of a CPACE application has the value 0b, every *Issuer Options Profile Control x* of the application shall have a length of 7 bytes.

If 'Allow Extended Controls' in the *Application Control* of a CPACE application has the value 1b, every *Issuer Options Profile Control x* of the application shall have a length of 7 or 10 bytes.

Note:

If an *Issuer Options Profile Control x* has a length of 7 bytes, it will be padded implicitly with 3 trailing bytes '00' to a length of 10 bytes and it will be used in the same way as an *Issuer Options Profile Control x* with a length of 10 bytes where bytes 8 to 10 have the value '00' (see Req C.47).

In this way processing of the *Issuer Options Profile Control* will be the same irrespective of the value of 'Allow Extended Controls' in the *Application Control*.

Issuer Options Profile Control x is coded as shown in Table 68.

Byte	Data Element	Description
1	Issuer Options Profile Parameters	See Table 69
2	First GENERATE AC Command Data Length	Length of the command data to be sent in the first GENERATE AC command message. The tags and lengths of these data elements were sent to the Terminal in CDOL1. The value of First GENERATE AC Command Data Length must be consistent with the contents personalised in CDOL1.
3	Second GENERATE AC Command Data Length	Length of the command data to be sent in the second GENERATE AC command message. The tags and lengths of these data elements were sent to the Terminal in CDOL2. The value of Second GENERATE AC Command Data Length must be consistent with the contents personalised in CDOL2.
4	Profile CCI	Profile CCI indicates the value to be used for the Common Core Identifier (CCI) in the profile.
5	Profile DKI	Profile DKI indicates the value to be used for the Derivation Key Index (DKI) in the profile.
6	RFU	
7 (- 10)	Proprietary Issuer Options Profile Parameters	See Table 70

Table 68: *Issuer Options Profile Control x* Coding

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	-	-	-	-	-	-	-	Log Transactions
0	-	-	-	-	-	-	-	Do Not Log Transactions
1	-	-	-	-	-	-	-	Log Transactions
-	1	-	-	-	-	-	-	Activate Additional Check Table 1 Check
-	-	1	-	-	-	-	-	Activate Additional Check Table 2 Check
-	-	-	1	-	-	-	-	Activate Maximum Number of Days Offline Check
-	-	-	-	1	-	-	-	Reset Maximum Number of Days Offline with Online Response
-	-	-	-	-	1	-	-	Allow Override of CIAC-Default for Transactions at Terminal Type 26
-	-	-	-	-	-	1	-	Encipher Counters Portion of IAD
-	-	-	-	-	-	-	x	RFU

Table 69: Issuer Options Profile Parameters

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	1	-	-	-	-	-	-	-	**Include Offline Transactions End Date in IAD**
	-	1	-	-	-	-	-	-	**Include Static Issuer Data in IAD**
	-	-	1	-	-	-	-	-	**Include Dynamic Issuer Data in IAD**
	-	-	-	1	-	-	-	-	**Use Issuer Discretionary Bits in CVR**
	-	-	-	-	1	-	-	-	**Proprietary Authentication Data in IATD Supported**
	-	-	-	-	-	x	-	-	**RFU**
	-	-	-	-	-	-	1	-	**Activate Cashback Check**
	-	-	-	-	-	-	-	x	**RFU**
2	x	x	x	x	x	x	x	x	**RFU**
3	1	-	-	-	-	-	-	-	**Relay Resistance Protocol Supported**[16)]
	-	x	x	x	x	x	x	-	**RFU**
	-	-	-	-	-	-	-	x	**Mode of AES Encipherment**[17)]
	-	-	-	-	-	-	-	0	**Encipher only Counters**
	-	-	-	-	-	-		1	**Encipher Counters and IDD**
4	x	x	x	x	x	x	x	x	**RFU**

Table 70: Proprietary Issuer Options Profile Parameters

21.43 *Log Data Tables*

Template: -
Tag: 'BF40'
Length (in bytes): var.
Format: b

Description: If the Internal Data Logging implementer-option is supported, the Log Data Tables template may contain an additional data object, the *Internal Log Data Object List (ILDOL)*.

21.44 *Master Key for AC*

Template: -
Tag: -
Length (in bytes): 16, if the Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option is supported also 24 or 32
Format: b

Description: *Master Key for AC* is the standard master key for Application Cryptogram generation in the standard set of master keys *Standard Master Keys*.

16) This bit applies only if the Relay Resistance Protocol implementer-option is supported.

17) This bit applies only if the CCI has the value 'A6' and if 'Encipher Counters Portion of IAD' bit is set to 1b.

21.45 *Master Key for SMC*

Template:	-
Tag:	-
Length (in bytes):	16, if the Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option is supported also 24 or 32
Format:	b
Description:	*Master Key for SMC* is the standard master key for Secure Messaging for Confidentiality in the standard set of master keys *Standard Master Keys*.

21.46 *Master Key for SMI*

Template:	-
Tag:	-
Length (in bytes):	16, if the Cryptogram Version '6'-only or Cryptogram Version '5' and '6' implementer-option is supported also 24 or 32
Format:	b
Description:	*Master Key for SMI* is the standard master key for Secure Messaging for Integrity in the standard set of master keys *Standard Master Keys*.

21.47 *Max Time For Processing Relay Resistance APDU*

Template:	-
Tag:	-
Length (in bytes):	2
Format:	b
Description:	This data element is only supported if the Relay Resistance Protocol implementer-option is supported. *Max Time For Processing Relay Resistance APDU* is a 2-byte binary value in units of hundreds of microseconds that represents the maximum time for processing the EXCHANGE RELAY RESISTANCE DATA command. *Max Time For Processing Relay Resistance APDU* is stored in bytes 3 to 4 of a *RRP Configuration Data Set*. During Relay Resistance Protocol Preparation (see Section 7.2.5), *Max Time For Processing Relay Resistance APDU* is retrieved from the *RRP Configuration Data Set* and stored transiently in bytes 11 to 12 of the *RRP Transaction Data Set* for inclusion in the EXCHANGE RELAY RESISTANCE DATA response message (see Section 8.2.4) and for inclusion in the generation of the dynamic signature (see Req C.99 in Section 12.2.7.4).

21.48 *Min Time For Processing Relay Resistance APDU*

Template: -
Tag: -
Length (in bytes): 2
Format: b

Description: This data element is only supported if the Relay Resistance Protocol implementer-option is supported.

Min Time For Processing Relay Resistance APDU is a 2-byte binary value in units of hundreds of microseconds that represents the minimum time for processing the EXCHANGE RELAY RESISTANCE DATA command.

Min Time For Processing Relay Resistance APDU is stored in bytes 1 to 2 of a *RRP Configuration Data Set*.

During Relay Resistance Protocol Preparation (see Section 7.2.5), *Min Time For Processing Relay Resistance APDU* is retrieved from the *RRP Configuration Data Set* and stored transiently in bytes 9 to 10 of the *RRP Transaction Data Set* for inclusion in the EXCHANGE RELAY RESISTANCE DATA response message (see Section 8.2.4) and for inclusion in the generation of the dynamic signature (see Req C.99 in Section 12.2.7.4).

21.49 *Profile Control*

Template: -
Tag: -
Length (in bytes): 10
Format: b

Description: *Profile Control* is the *Profile Control x* selected for the transaction according to Section 7.2.3 of this document and according to Req 8.12 in Section 8.5.4.1 of [CPA].

21.50 *Profile Control x*

Template:	'BF3F'
Tag:	'DFxx'
Length (in bytes):	8 **or 10**
Format:	b

Description: *Profile Control x* is a list of resource IDs and resource control IDs that identify the Profile-specific data and behaviour when processing a transaction using *Profile ID* x.

x may have any value between 1 and 126 and is coded in the second byte of the tag 'DFxx'.

Bytes 1 to 6 of *Profile Control x* are defined by [CPA]. Bytes 7 to 10 are defined by this specification.

If the Additional Master Keys implementer-option is not supported, then 'Master Keys ID' (bits b8-b5 of byte 7) in *Profile Control x* shall be set to '0'.

If the Additional Master Keys implementer-option is supported, then 'Master Keys ID' in *Profile Control x* shall be used as follows:

- 'Master Keys ID' = '0' indicates that the Additional Master Keys function is switched off and that the standard CPA master keys shall be used for the profile.
- 'Master Keys ID' = 'x' <> '0' indicates that the Additional Master Keys function is switched on and that the master keys with identifier 'x' shall be used for the profile.

Note:

If the EMV CPS implementer-option is supported, then 'Master Keys ID' = 'x' <> '0' refers to the value 'x' in DGIs '840x' and '940x' for Triple DES keys or in DGIs '841x' and '941x' for AES.

If 'Use Additional Accumulators and Counter' (byte 4, bit b3) in the *Application Control* of a CPACE application has the value 0b, every *Profile Control x* of the application shall have a length of 8 bytes.

If 'Use Additional Accumulators and Counter' in the *Application Control* of a CPACE application has the value 1b, every *Profile Control x* of the application shall have a length of 10 bytes.

Note:

If a *Profile Control x* has a length of 8 bytes, it will be padded implicitly with 2 trailing bytes 'FF' to a length of 10 bytes and used in the same way as a *Profile Control x* with a length of 10 bytes where bytes 9 and 10 have the value 'FF' (see Req C.46).

In this way the processing of the *Profile Control* will be the same irrespective of the value of 'Use Additional Accumulators and Counter' in the *Application Control*.

Profile Control x is coded as shown in Table 71.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	-	-	-	-	Issuer Options Profile Control ID
	-	-	-	-	x	x	x	x	AIP/AFL ID
2	x	x	x	x	-	-	-	-	CIACs ID
	-	-	-	-	x	x	x	x	Accumulator 1 Profile Control ID
3	x	x	x	x	-	-	-	-	Accumulator 2 Profile Control ID
	-	-	-	-	x	x	x	x	Counter 1 Profile Control ID
4	x	x	x	x	-	-	-	-	Counter 2 Profile Control ID
	-	-	-	-	x	x	x	x	Counter 3 Profile Control ID
5	x	x	x	x	-	-	-	-	Cyclic Accumulator 1 Profile Control ID
	-	-	-	-	x	x	x	x	Cyclic Accumulator 2 Profile Control ID
6	x	x	x	x	-	-	-	-	MTA (Max. Transaction Amount) Profile Control ID
	-	-	-	-	1	1	1	1	Not used[18)]
7	x	x	x	x	-	-	-	-	**Master Keys ID**
	-	-	-	-	x	x	x	x	RFU
8	x	x	x	x	x	x	x	x	RFU
9	x	x	x	x	-	-	-	-	**Accumulator 3 Profile Control ID**
	-	-	-	-	x	x	x	x	**Counter 4 Profile Control ID**
10	1	1	1	1	-	-	-	-	**Not used**
	-	-	-	-	x	x	x	x	**RFU**

Table 71: *Profile Control x* Coding

18) Since VLP is not supported in the CPACE application, this field is set to 'F' to indicate it is not used, as required by [CPA].

21.51 *Profile Selection Entry*

Template: -
Tag: -
Length (in bytes): var.
Format: b

Description: Each record of the Profile Selection File (see Section 9.7.3 of [CPA]) contains a *Profile Selection Entry* without a record template tag.

According to this specification, the coding of a *Profile Selection Entry* depends on the value of 'Allow Profile Selection with Extended Check Types' (byte 4, bit b2) in the *Application Control* of the CPACE application:

- If 'Allow Profile Selection with Extended Check Types' in the *Application Control* has the value 0b, all *Profile Selection Entries* in the records of the Profile Selection File may only contain one of the Check Types '00', '01' and '02' and shall be coded as shown for these Check Types in Table 72, Table 73 and Table 75.
- If 'Allow Profile Selection with Extended Check Types' bit in the *Application Control* has the value 1b, the *Profile Selection Entries* in the records of the Profile Selection File may contain one of the Extended Check Types defined in Table 74 or one of the Check Types '00', '01' and '02' and shall be coded as shown for these Check Types in Table 72, Table 73 and Table 75.

The coding of a *Profile Selection Entry* as shown in Table 72, Table 73 and Table 75 with Check Types '00', '01' and '02' is defined by [CPA].

The coding of a *Profile Selection Entry* as shown in Table 72, Table 73 and Table 75 with Extended Check Types shown in Table 74 is defined by this specification.

A *Profile Selection Entry* may be shorter than the record of the Profile Selection File the *Profile Selection Entry* is stored in (see section 9.5.3 of [CPA]). In this case the *Profile Selection Entry* shall be stored left adjusted in the record with trailing filler bytes '00' at the end of the record.

Position	Data Element	Length (in bytes)	Format	Description
Byte 1	Entry Length	1	b	Profile Selection Entry length (not including the Entry Length)
Byte 2	Position P in Extended GPO Input Data	1	b	A value greater than '00' indicates the position of the first byte of data extracted from the Extended GPO Input Data that is compared to the comparison values listed in this Profile Selection Entry. If the first byte in the first Extended GPO Input Data is extracted for comparison, the value of P is '01'. The value '00' It indicates that no data shall be extracted from the Extended GPO Input Data. The value '00' is not allowed for Check Types '00', '01', '02'. It is only allowed for Extended Check Types (bit b8 of the Check Type has the value 1b) which do not require the Transaction Amount (bit b7 or bit b2 of the Extended Check Type has the value 0b).
Byte 3	Length L of Extraction Block and/or Comparison Block	1	b	If data is to be extracted from the Extended GPO Input Data (the value of P in byte 2 is greater than '00') the value of byte 3 shall be greater than '00' and indicates the length L in bytes of the data to be extracted from the Extended GPO Input Data. If comparison blocks are to be used (the value of byte 4 is greater than '00') the value of byte 3 shall be greater than '00' and indicates the length L in bytes of the comparison value(s). If byte 2 and byte 4 of the Profile Selection Entry have the value '00' the value of byte 3 is not evaluated and should be set to '00'

Position	Data Element	Length (in bytes)	Format	Description
Byte 4	Number n of Comparison Blocks	1	b	The number n of comparison blocks in this Profile Selection Entry. A value greater than or equal to '02' indicates that the first comparison block is a bit mask and that the second and subsequent comparison block(s) are comparison values that are compared to the data extracted from Extended GPO Input Data. The value '00' indicates that no comparison blocks are used. The value '01' indicates that no bit mask and only one comparison block is used. The values '00' and '01' are not allowed for Check Types '00', '01', '02'. They are only allowed for Extended Check Types (bit b8 of the Check Type has the value 1b).
Bytes 5 - 4+n*L	Comparison Blocks	var.	b	Comparison Blocks are only present if n (and therefore also L) is greater than 0. For the coding of Comparison Blocks, see Table 73

Position	Data Element	Length (in bytes)	Format	Description
Byte n*L+5	Check Type	1	b	Identifies the type of test to be performed using the masked data extracted from the Extended GPO Input Data and the comparison value(s). If bit b8 of the Check Type has the value 0b the Check Type is identified as follows: **Match (Check Type = '00')** Tests whether the masked value extracted from the Extended GPO Input Data is **equal to** any of the comparison values in this Profile Selection Entry. **Less Than (Check Type = '01')** Tests whether the masked value extracted from the Extended GPO Input Data is **less than** comparison value 1 in this Profile Selection Entry. **Greater Than (Check Type = '02')** Tests whether the masked value extracted from the Extended GPO Input Data is **greater than** comparison value 1 in this Profile Selection Entry. If bit b8 of the Check Type has the value 1b the Check Type is an Extended Check Type coded as shown in Table 74.
Byte n*L+6	Positive Action	1	b	Action to be taken when the Check Type test is **true**. See Table 75
Byte n*L+7	Negative Action	1	b	Action to take when the Check Type test is **false**. See Table 75

Table 72: *Profile Selection Entry* Coding

Position	Data Element	Length (in bytes)	Format	Description
Bytes 1 - L	Bit Mask	L	b	Used to mask the data extracted from the Extended GPO Input Data, allowing the comparison to be based on a portion of the extracted data. Set to 0b for each bit that is not used in the comparison, and set to 1b for each bit that is used in the comparison.
Bytes L+1 - 2*L	Comparison Value 1	L	b	The first value compared to the masked data extracted from the Extended GPO Input Data.
…	…	…	…	…
Bytes (n-1)*L+1 - n*L	Comparison Value n-1	L	b	The last value compared to the masked data extracted from the Extended GPO Input Data.

Table 73: Comparison Blocks Coding

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	Extended Check Type
-	x	-	-	-	-	-	-	Use Accumulator or Counter
-	1	-	-	-	-	-	-	Use Accumulator
-	0	-	-	-	-	-	-	Use Counter
-	-	x	x	-	-	-	-	Accumulator or Counter Number (00b not allowed for Accumulators, refers to Counter 4 for Counters)
-	-	-	-	x	-	-	-	Limit Set ID (not evaluated and should be set to 0b if n > 0, i.e. if Comparison Value used)
-	-	-	-	-	x	-	-	Lower/Upper Limit (not evaluated and should be set to 0b if n > 0, i.e. Comparison Value used)
-	-	-	-	-	1	-	-	Upper Limit
-	-	-	-	-	0	-	-	Lower Limit
-	-	-	-	-	-	x	-	Add Transaction (Amount)
-	-	-	-	-	-	1	-	Add Transaction (Amount) to Accumulator/Counter
-	-	-	-	-	-	0	-	Do Not Add Transaction (Amount) to Accumulator/Counter
-	-	-	-	-	-	-	x	Less/Greater Than
-	-	-	-	-	-	-	1	Tests whether the Accumulator (+ Transaction Amount) or the Counter (+ 1) is **greater than** comparison value 1 or Limit
-	-	-	-	-	-	-	0	Tests whether the Accumulator (+ Transaction Amount) or the Counter (+ 1) is **less than** comparison value 1 or Limit

Table 74: Extended Check Type Coding

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	-	-	-	-	-	-	-	Meaning of bits b7 - b1
0	-	-	-	-	-	-	-	Select *Profile ID*
1	-	-	-	-	-	-	-	Move down in Profile Selection File
-	x	x	x	x	x	x	x	*Profile ID* (b8 = 0) or Number of Profile Selection Entries to move down in the Profile Selection File for the next Profile Selection Entry to process (b8 = 1)

Table 75: Positive and Negative Action Byte Coding

21.52 *Proprietary Authentication Data (PAD)*

Template: -
Tag: -
Length (in bytes): 8
Format: b

Description: *Proprietary Authentication Data (PAD)* may be sent from the issuer or its proxy to the CPACE application in bytes 9-16 of *Issuer Authentication Data (IATD)* (see Section 21.40).

Proprietary Authentication Data (PAD) are defined by this specification. *Proprietary Authentication Data (PAD)* are coded as shown in Table 76.

Position	Data Element	Length (in bytes)	Format
Byte 1	Update Counters Byte (see Table 77)	1	b
	or filler[19)]		
Bytes 2 - 3	Number of Days Offline Limit	2	n 4
	or filler[19)]		b
Bytes 4 - 8	Accumulator 1 Upper Limit	5	n 10
	or filler[19)]		b

Table 76: *Proprietary Authentication Data (PAD)* Coding

19) Filler bytes contained in the *PAD* may have any value or format. Therefore, filler bytes are considered to have the format b (binary).

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	-	-	-	-	-	-	Update Counter 1
0	0	-	-	-	-	-	-	Do Not Update Counter 1
0	1	-	-	-	-	-	-	Set Counter 1 to Upper Limit
1	0	-	-	-	-	-	-	Reset Counter 1 to Zero
1	1	-	-	-	-	-	-	Add Transaction to Counter 1
-	-	x	x	-	-	-	-	Update Counter 2
-	-	0	0	-	-	-	-	Do Not Update Counter 2
-	-	0	1	-	-	-	-	Set Counter 2 to Upper Limit
-	-	1	0	-	-	-	-	Reset Counter 2 to Zero
-	-	1	1	-	-	-	-	Add Transaction to Counter 2
-	-	-	-	x	x	-	-	Update Counter 3
-	-	-	-	0	0	-	-	Do Not Update Counter 3
-	-	-	-	0	1	-	-	Set Counter 3 to Upper Limit
-	-	-	-	1	0	-	-	Reset Counter 3 to Zero
-	-	-	-	1	1	-	-	Add Transaction to Counter 3
-	-	-	-	-	-	x	x	Update Counter 4
-	-	-	-	-	-	0	0	Do Not Update Counter 4
-	-	-	-	-	-	0	1	Set Counter 4 to Upper Limit
-	-	-	-	-	-	1	0	Reset Counter 4 to Zero
-	-	-	-	-	-	1	1	Add Transaction to Counter 4

Table 77: Update Counters Byte Coding

21.53 *RRP Configuration Data Set*

Template: -
Tag: -
Length (in bytes): 6
Format: b

Description: If the Relay Resistance Protocol implementer-option is supported, each record of the RRP Configuration File (see Section 9.3.3.3) contains an *RRP Configuration Data Set* without a record template tag.

An *RRP Configuration Data Set* contains the timing information which is passed to the terminal for performing the Relay Resistance Protocol. An *RRP Configuration Data Set* is coded as shown in Table 78.

Note:

Currently, only one *RRP Configuration Data Set* and therefore only one record in the RRP Configuration File is needed which is used for performing the Relay Resistance Protocol over the contactless interface.

An *RRP Configuration Data Set* may be shorter than the record of the RRP Configuration File the *RRP Configuration Data Set* is stored in (see Section 9.3.3.3). In this case the *RRP Configuration Data Set* shall be stored left adjusted in the record with trailing filler bytes '00' at the end of the record.

Position	Data Element	Length (in bytes)	Format
Bytes 1 - 2	*Min Time For Processing Relay Resistance APDU*	2	b
Bytes 3 - 4	*Max Time For Processing Relay Resistance APDU*	2	b
Bytes 5 - 6	*Device Estimated Transmission Time For Relay Resistance R-APDU*	2	b

Table 78: *RRP Configuration Data Set* Coding

21.54 *RRP Configuration File Entry*

Template: -
Tag: 'D9'
Length (in bytes): 2
Format: b

Description: This data element is only supported if the Relay Resistance Protocol implementer-option is supported.

Devices that read the RRP Configuration File from a CPACE application use the *RRP Configuration File Entry* to determine the location (SFI) and the maximum number of records to be read (that is, the maximum number of *RRP Configuration Data Sets*) in the file. The actual number of *RRP Configuration Data Sets* in the RRP Configuration File may be less than the maximum number indicated in the *RRP Configuration File Entry*.

The *RRP Configuration File Entry* is coded as shown in Table 79.

The *RRP Configuration File Entry* may be obtained from the application using the GET DATA command, but cannot be updated using the PUT DATA command.

Note:

Coding of the *RRP Configuration File Entry* has to be consistent with the actual parameters of the RRP Configuration File the in which the *RRP Configuration Data Sets* are stored. Changing the *RRP Configuration File Entry* does not change the location and size of the RRP Configuration File.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	-	-	-	SFI of the RRP Configuration File
	-	-	-	-	-	x	x	x	RFU
2	x	x	x	x	x	x	x	x	Maximum number of *RRP Configuration Data Sets* in the RRP Configuration File

Table 79: *RRP Configuration File Entry* Coding

21.55 *RRP Counter*

Template: -
Tag: -
Length (in bytes): 1
Format: b

Description: This data element is only supported if the Relay Resistance Protocol implementer-option is supported.

RRP Counter is an internal parameter of the CPACE application which is reset by the GET PROCESSING OPTIONS command (see Req C.44) and counts the number of EXCHANGE RELAY RESISTANCE DATA commands after a GET PROCESSING OPTIONS command (see Section 8.2.3).

21.56 *RRP Dynamic Number*

Template: -
Tag: -
Length (in bytes): 12
Format: b

Description: This data element is only supported if the Relay Resistance Protocol implementer-option is supported.

RRP Dynamic Number is a transiently stored 12-byte random number generated during Relay Resistance Protocol Preparation (see Section 7.2.5).

RRP Dynamic Number is used for he generation of the *Device Relay Resistance Entropy* in the response to the EXCHANGE RELAY RESISTANCE DATA command.

21.57 *RRP Transaction Data Set*

Template: -
Tag: -
Length (in bytes): 14
Format: b

Description: This data element is only supported if the Relay Resistance Protocol implementer-option is supported.

The *RRP Transaction Data Set* is an internal parameter of the CPACE application which is used to store transiently the data elements related to the Relay Resistance Protocol. The *RRP Transaction Data Set* is coded as shown in Table 80.

RRP Transaction Data Set is initialised during Relay Resistance Protocol Preparation (see Section 7.2.5).

Terminal Relay Resistance Entropy and *Device Relay Resistance Entropy* are added during EXCHANGE RELAY RESISTANCE DATA Command Processing (see Section 8.2.3).

Bytes 5 to 15 of the *RRP Transaction Data Set* are returned in the response to the EXCHANGE RELAY RESISTANCE DATA command.

All of *RRP Transaction Data Set* is included in the generation of the dynamic signature (see Req C.99 in Section 12.2.7.4).

Position	**Data Element**	**Length** (in bytes)	**Format**
Bytes 1 - 4	*Terminal Relay Resistance Entropy*	4	b
Bytes 5 - 8	*Device Relay Resistance Entropy*	4	b
Bytes 9 - 10	*Min Time For Processing Relay Resistance APDU*	2	b
Bytes 11 - 12	*Max Time For Processing Relay Resistance APDU*	2	b
Bytes 13 - 14	*Device Estimated Transmission Time For Relay Resistance R-APDU*	2	b

Table 80: *RRP Transaction Data Set* Coding

21.58 *Security Limits*

Template: -
Tag: 'C5'
Length (in bytes): 6
Format: b

Description: *Security Limits* is supported when the Application Security Counters implementer-option (see Section 18) is supported.

Security Limits is coded as shown in Table 81.

If supported, *Security Limits* are not retrievable from the application and may be updated using the PUT DATA command.

	For DDA or CDA applications	**For SDA-only applications**
Byte	**Data Element**	**Data Element**
1 - 2	*AC Session Key Counter Limit*	*AC Session Key Counter Limit*
3 - 4	*SMI Session Key Counter Limit*	*SMI Session Key Counter Limit*
5 - 6	*PIN Decipherment Error Counter Limit*	'00 00'

Table 81: *Security Limits* Coding

21.59 *Security Limits Status*

Template: -
Tag: 'C4'
Length (in bytes): 1
Format: b

Description: *Security Limits Status* is supported when the Application Security Counters implementer-option (see Section 18) is supported.

Security Limits Status is coded as shown in Table 82.

The value of this data element indicates for the standard *Master Key for AC*, for the standard *Master Key for SMI* and for the PIN decipherment private key whether the limit for a security counter that limits the number of times the respective key is used has been reached.

If supported, *Security Limits Status* may be retrieved from the application using the GET DATA command, but cannot be updated with the PUT DATA command.

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	-	-	-	-	-	-	-	*AC Session Key Counter Limit* exceeded
-	1	-	-	-	-	-	-	*SMI Session Key Counter Limit* exceeded
-	-	1	-	-	-	-	-	*PIN Decipherment Error Counter Limit* exceeded
-	-	-	x	x	x	-	-	RFU
-	-	-	-	-	-	x	x	Issuer Proprietary

Table 82: *Security Limits Status* Coding

21.60 *SMI Session Key Counter*

Template: -
Tag: -
Length (in bytes): 2
Format: b

Description: *SMI Session Key Counter* is supported when the Application Security Counters implementer-option is supported (see Section 18).

SMI Session Key Counter is the internal counter defined in [CPA] that counts the number of Secure Messaging for Integrity session key derivations using *Master Key for SMI* that are not followed by successful validation of a Secure Messaging MAC, over the lifetime of the CPACE application.

21.61 *SMI Session Key Counter Limit*

Template: -
Tag: -
Length (in bytes): 2
Format: b

Description: *SMI Session Key Counter Limit* is supported when the Application Security Counters implementer-option is supported (see Section 18).

SMI Session Key Counter Limit is the limit defined in [CPA] that limits the number of Secure Messaging for Integrity session key derivations using *Master Key for SMI* that are not followed by successful validation of a Secure Messaging MAC, over the lifetime of the CPACE application.

21.62 *Standard Master Keys*

Template: -
Tag: -
Length (in bytes): var.
Format: b

Description: *Standard Master Keys* denotes the standard set of symmetric master keys which has to be supported by a CPACE application according to [CPA].

Standard Master Keys consists of the standard master keys *Master Key for AC*, *Master Key for SMC* and *Master Key for SMI* described in [CPA].

If the Cryptogram Version '5'-only implementer-option is supported, *Standard Master Keys* is a set of Triple DES keys, each with a length of 16 bytes.

If the Cryptogram Version '6'-only implementer-option is supported, *Standard Master Keys* is a set of AES keys, each with the same length of either 16, 24 or 32 bytes.

If the Cryptogram Version '5' and '6' implementer-option is supported, *Standard Master Keys* is either a set of Triple DES keys, each with a length of 16 bytes, or a set of AES keys, each with the same length of either 16, 24 or 32 bytes.

21.63 *Static Issuer Data*

Template: -
Tag: 'D0'
Length (in bytes): var.
Format: b

Description: Issuer specific static data. The value of the *Static Issuer Data* will be included in the Issuer Discretionary Data of the *Issuer Application Data*, if 'Include Static Issuer Data in IAD' (byte 7, bit b7) has the value 1b in the *Issuer Options Profile Control*.

Static Issuer Data may be obtained from the application using the GET DATA command and may be updated using the PUT DATA command.

21.64 *Terminal Relay Resistance Entropy*

Template: -
Tag: -
Length (in bytes): 4
Format: b

Description: This data element is only supported if the Relay Resistance Protocol implementer-option is supported.

Terminal Relay Resistance Entropy is a 4-byte (random) number provided by the terminal in the command data field of the EXCHANGE RELAY RESISTANCE DATA command.

During EXCHANGE RELAY RESISTANCE DATA Command Processing (see Section 8.2.3), the *Terminal Relay Resistance Entropy* is stored transiently in bytes 1 to 4 of the *RRP Transaction Data Set* for inclusion in the generation of the dynamic signature (see Req C.99 in Section 12.2.7.4).

21.65 *Terminal Risk Management Data*

Template: -
Tag: '9F1D'
Length (in bytes): 8
Format: b

Description: *Terminal Risk Management Data* is an EMV terminal data object the format of which is application specific.

For usage with the CPACE application it is coded as shown in Table 83.

Though a tag is defined for *Terminal Risk Management Data*, it cannot be obtained from the application using the GET DATA command and cannot be updated using the PUT DATA command.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	1	-	-	-	-	-	-	-	Restart supported
	-	1	-	-	-	-	-	-	Enciphered PIN verified online (Contactless)
	-	-	1	-	-	-	-	-	Signature (paper) (Contactless)
	-	-	-	1	-	-	-	-	Enciphered PIN verification performed by ICC (Contactless)
	-	-	-	-	1	-	-	-	No CVM required (Contactless)
	-	-	-	-	-	1	-	-	On device cardholder verification (Contactless)
	-	-	-	-	-	-	1	-	Plaintext PIN verification performed by ICC (Contactless)
	-	-	-	-	-	-	-	1	Present and Hold supported

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
2	x	-	-	-	-	-	-	-	RFU
	-	1	-	-	-	-	-	-	Enciphered PIN verified online (Contact)
	-	-	1	-	-	-	-	-	Signature (paper) (Contact)
	-	-	-	1	-	-	-	-	Enciphered PIN verification performed by ICC (Contact)
	-	-	-	-	1	-	-	-	No CVM required (Contact)
	-	-	-	-	-	1	-	-	On device cardholder verification (Contact)
	-	-	-	-	-	-	1	-	Plaintext PIN verification performed by ICC (Contact)
	-	-	-	-	-	-	-	x	RFU
3	1	-	-	-	-	-	-	-	Mag-Stripe-Mode contactless transactions not supported
	-	1	-	-	-	-	-	-	EMV-Mode contactless transactions not supported
	-	-	x	x	x	x	x	x	RFU
4	x	x	x	x	x	x	x	x	RFU
5	x	x	x	x	x	x	x	x	RFU
6	x	x	x	x	x	x	x	x	RFU
7	x	x	x	x	x	x	x	x	RFU
8	x	x	x	x	x	x	x	x	RFU

Table 83: *Terminal Risk Management Data*

21.66 *Terminal Verification Results (TVR)*

Template: -
Tag: '95'
Length (in bytes): 5
Format: b

Description: *Terminal Verification Results (TVR)* indicate the status of the different functions as seen from the terminal as defined in [EMV 3].

In addition to the definition in [EMV 3], bits b4 through b1 of byte 5 that have been reserved for use by contactless specifications indicate the status of the Relay Resistance Protocol as seen from the terminal.

Terminal Verification Results (TVR) are coded as shown in Table 84.

Though a tag is defined for *Terminal Verification Results (TVR)*, it cannot be obtained from the application using the GET DATA command and cannot be updated using the PUT DATA command.

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	1	-	-	-	-	-	-	-	Offline data authentication was not performed
	-	1	-	-	-	-	-	-	SDA failed
	-	-	1	-	-	-	-	-	ICC data missing
	-	-	-	1	-	-	-	-	Card appears on terminal exception file
	-	-	-	-	1	-	-	-	DDA failed
	-	-	-	-	-	1	-	-	CDA failed
	-	-	-	-	-	-	x	x	RFU
2	1	-	-	-	-	-	-	-	ICC and terminal have different application versions
	-	1	-	-	-	-	-	-	Expired application
	-	-	1	-	-	-	-	-	Application not yet effective
	-	-	-	1	-	-	-	-	Requested service not allowed for card product
	-	-	-	-	1	-	-	-	New card
	-	-	-	-	-	x	x	x	RFU
3	1	-	-	-	-	-	-	-	Cardholder verification was not successful
	-	1	-	-	-	-	-	-	Unrecognised CVM
	-	-	1	-	-	-	-	-	PIN Try Limit exceeded
	-	-	-	1	-	-	-	-	PIN entry required and PIN pad not present or not working
	-	-	-	-	1	-	-	-	PIN entry required, PIN pad present, but PIN was not entered
	-	-	-	-	-	1	-	-	Online PIN entered
	-	-	-	-	-	-	x	x	RFU
4	1	-	-	-	-	-	-	-	Transaction exceeds floor limit
	-	1	-	-	-	-	-	-	Lower consecutive offline limit exceeded
	-	-	1	-	-	-	-	-	Upper consecutive offline limit exceeded
	-	-	-	1	-	-	-	-	Transaction selected randomly for online processing
	-	-	-	-	1	-	-	-	Merchant forced transaction online
	-	-	-	-	-	x	x	x	RFU
5	1	-	-	-	-	-	-	-	Default TDOL used
	-	1	-	-	-	-	-	-	Issuer authentication failed
	-	-	1	-	-	-	-	-	Script processing failed before final GENERATE AC
	-	-	-	1	-	-	-	-	Script processing failed after final GENERATE AC
	-	-	-	-	1	-	-	-	Relay resistance threshold exceeded
	-	-	-	-	-	1	-	-	Relay resistance time limits exceeded
	-	-	-	-	-	-	x	x	Relay Resistance Protocol performed
	-	-	-	-	-	-	0	0	RRP not supported
	-	-	-	-	-	-	0	1	RRP not performed
	-	-	-	-	-	-	1	0	RRP performed
	-	-	-	-	-	-	1	1	RFU

Table 84: *Terminal Verification Results (TVR)* Coding

21.67 *Third Party Data*

Template: 'BF0C' or '70'
Tag: '9F6E'
Length (in bytes): 5-32
Format: b

Description: *Third Party Data* contains various information, possibly including information from a third party. If present in the card, *Third Party Data* must be returned in a file read using the READ RECORD command or in the *FCI Issuer Discretionary Data* template.

Third Party Data is coded as shown in Table 85.

'Device Type' is present when the most significant bit of byte 1 of 'Unique Identifier' is set to 0b. In this case, the maximum length of 'Proprietary Data' is 26 bytes. Otherwise it is 28 bytes.

Data Field	Length (in bytes)	Format	Value
Country Code	2	n 3	Country Code according to [ISO 3166-1]
Unique Identifier	2	b	Value assigned by the scheme
Device Type	0 or 2	an	
Proprietary Data	1-26 or 28	b	

Table 85: *Third Party Data* Coding

21.68 *Transaction CVM*

Template: -
Tag: -
Length (in bytes): 1
Format: b

Description: *Transaction CVM* is an internal parameter of the CPACE application which is used to store the CVM with which cardholder verification was performed.

'01' Offline PIN (successfully verified)
'02' Online PIN (selected for cardholder verification)
'03' Signature (selected for cardholder verification)
'00' No CVM (none of the above)

All other values RFU

Determination of *Transaction CVM* is described in Section 12.2.3.2.

Note:

According to this definition, *Transaction CVM* has the value No CVM, if cardholder verification was not performed or failed, or if cardholder verification was successfully performed using No CVM Required as CVM.