NATIONAL COMMON MOBILITY CARD

MINIMUM STANDARDS & SPECIFICATION DOCUMENT FOR CARD AND DEVICES

Document prepared and owned by	*UTIITSL*
Date	*20th April 2012*
Version	*Version 01 Release 06*

Table of Contents

Copyright © UTIITSL NCMC Project

Table of Figures

Copyright © UTIITSL NCMC Project

FOREWORD

This specification and standards document has been prepared by UTIITSL, its Consortium Partners after multiple discussions with industry experts, technology providers and partners and stakeholders. It has been written to be compatible with the requirements of National and International Standards.

The specification can be used for the standardization of devices and recommended to be

used for the implementation of National Common Mobility Program in the multi modal and multi-operator environment within the practical limits for transport.

This document provides minimum standards and specification of the card and essential devices to implement National Common Mobility Card Program.

The essential standards & specifications of devices and card details available in this document are intended for the National Common Mobility Card Program. The use of these standards for applications other than their intended use may require adjustment to meet all applicable criteria. Those parties using these Standards & Specifications details are responsible for due diligence prior to their use.

It is important that sufficient information is provided to the public transport Organization or implementing agency.

Copyright © UTIITSL NCMC Project

DISCLAIMER

Any diversion or misinterpretation from the content of this document and its subsequent consequences will be the responsibility of the user of this document.

UTIITSL, its consortium partners, technology partners, industry experts, stakeholders, and employees do not endorse any product make or brand as per the specification mentioned in this Document.

UTIITSL, its consortium partners, technology partners, industry experts, stakeholders and employees do not provide any warranty of the item whatsoever, whether express, implied, or statutory, including, but not limited to, any warranty of merchantability or fitness for a particular purpose or any warranty that the contents of the item will be error-free.

In no respect shall UTIITSL, its consortium partners, technology partners, industry experts, stakeholders and employees incur any liability for any damages, including, but not limited to, direct, indirect, special, or consequential damages arising out of, resulting from, or any way connected to the use of the item, whether or not based upon warranty, contract, tort, or otherwise; whether or not injury was sustained by persons or property or otherwise; and whether or not loss was sustained from, or arose out of, the results of, the item, or any services that may be provided by UTIITSL.

© COPYRIGHT PROTECTED DOCUMENT

All rights reserved unless otherwise specified. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilming, without written permission from UTIITSL.

1 VISION OF THE DOCUMENT

This document is intended to define and establish a set of open and national standards for all devices to be used as a part of the National Common Mobility Card Project. This would help to achieve a well defined platform for successful implementation of the NCMC nationwide.

2 INTRODUCTION

The National Common Mobility Card (NCMC), based on the Contactless Smart Card (CSC) technology has been chosen as the solution to provide a multi-purpose common fare / ticket media across different operators (both Government and private) as an integrated approach for the utmost convenience of the common man. For the operators, such a system will be efficient, cost effective, dynamic and robust.

Some major aspects of multi-modal and multi-operator seamless connectivity are fare / ticket media integration and effective clearance & settlement. Contemporary technology makes it feasible to provide fare / ticket media integration in the form of a common fare / ticket media by means of the National Common Mobility Card (NCMC) which can work as per the fare system of any issuing operator and as a common e-purse to enable ticketing on other operators' network.

On a national scale it will be ruled by certain specifications and adhere to some common standards to make the interoperability seamless and technically possible. It is envisaged that a single agency should take responsibility for coordination to make this successful through common planning and management of the solution. To ensure the success of seamless travel for the commuters in India, there is a prerequisite that common standards be adopted at the national level, between PTOs, including those collecting fares for transit services. The various standards including equipment and interface specifications will be issued by UTIITSL on behalf of MoUD to make the interoperability seamless and technically feasible.

NCMC will include a large set and subset of different equipments that shall be used for varied purposes. This includes devices that are directly linked to automatic ticketing such as fare collection devices like Electronic Ticketing Machines and Smart Card Validators or other equipment like Public Information Systems, Integrated Control Units, CCTV cameras, Vehicle Tracking System etc.

Copyright © UTIITSL NCMC Project

3 ADVANTAGES / DISADVANTAGES OF USING E-TICKETING STANDARDISED PRODUCTS

Referring to standards when defining e-ticketing specifications offer several advantages in terms of sustainability of systems, modularity of its components, interoperability of systems, provision of information to travelers, cost saving, etc. However, these benefits will be lesser when technological evolution will imply to replace equipments or some part of them. The table below summarizes the main advantages of opting for standardized systems, according to each type of stakeholder.

STAKE HOLDER	ADVANTAGES
Public Transport Authorities	• Nation-wide common technical specifications • Better use of financial resources • More potential bidders (choices) • Compliance of bids • Free from any industrial interest
Public transport operators	• Continuity and easy integration of existing equipment with new one • Optimisation of acquisition and maintenance costs
Industry suppliers	• Benefit from standardisation • Ensure interoperability • Market opening • Less specific orders • Return on initial investment

Copyright © UTIITSL NCMC Project

4 DEVELOPMENT APPROACH

To achieve the objective of development and adoption of common standards at the national level, a structured approach towards NCMC was exercised. This was necessary for a systematic and streamlined process. One of the fundamental requirements of structured approach was to ensure that the output of the entire process results in a baseline document that defines the various standards, processes and specifications to be adhered for NCMC. These standards should incorporate and be derivates of international standardized certifications such as ISO, PCI and EMV for maintaining the highest and strictest control on quality and security of the system.

(a) Conceptualisation of NCMC

(b) Market research

(c) Feasibility study

(d) Information gathering, data collection and workshops

(e) Detailed Interactions and discussions with various stakeholders including international industry experts of the AFC domain

(f) Participating in International / National Events such as Urban Mobility India 2010 & 2011

(g) A round table discussion was held with all stakeholders at the UMI - 2010

(h) Drafting and outlining of NCMC standards, specifications and processes based on gathered data analysis and feedback from all stakeholders

(i) Continuous liaison with all stakeholders to achieve a functioning feedback chain

(j) Finalisation of set of standards and specifications

Copyright © UTIITSL NCMC Project

5 METHODOLOGY

The structured approach towards NCMC defined above was carried out with a methodical process.

The endeavour for the NCMC was started by initiating a detailed, in-depth market research and feasibility study to discover the scope and potential of a nationwide contactless smart card solution in the transit and para-transit services. This National Common Mobility Card would provide a common 'fare / ticket media' across multiple operators and multiple modes of transport across the nation. Fare / ticket media integration and efficient clearance & settlement for distributed parties would be the hallmark of this project. Concepts similar to the NCMC already exist world over with Oyster Card of London, Octopus of Hong Kong and EZ Crad of Singapore as some well known examples. NCMC however would be an entirely new scale.

As a part of the market research and study, comparisons were made with AFC solutions with devices existing in other countries, and correlating these to Indian context & requirements. As an example, one of the findings of this study was that although Fixed validation and ticketing devices are more popular in western countries, Indian conditions were more receptive to On-Board Validators and hand held Electronic Ticketing Machine. Hence, it was advisable to consider this option for NCMC. Several other findings were revealed during this stage of the methodology with the help of discussions, preparing questionnaires and interacting with several stakeholders of the project including the general public, PTOs, Railways, Metro, industry experts and SMEs.

Based on R&D with these stakeholders, a draft document was prepared along with some industry consultants and submitted to the Ministry of Urban Development (MoUD).

The above process enabled us to create an outline of the scope and architecture of the NCMC program. This was followed by another session of market research which was more focussed towards exploring various Products (devices) and solution options in the industry. Findings revealed a market abundant in various technology choices but to assure a secure and reliable system, standardised products with industry heritage and advanced security mechanisms were preferred. Being a financial transaction driven system and with future functionalities of banking card use, all devices installed as a part of NCMC should ideally be PCI as well as EMV certified. This is imperative to robustly secure and maintain the sanctity of all transactions generated and transmitted from and to these devices. A pivotal component for the security and protection of transactions and transaction devices is the Secure Access Module (SAM). The SAM cards would have to be interfaced to communicate with NCMC devices. For a standard NCMC program to be successful, specifications, functionality and interfaces for SAM have to be well defined (Appendix A). The SAM will be used only for NCMC applications, the functional behaviour of this would be totally customized to suite this application requirement. This shall

Copyright © UTIITSL NCMC Project

perform all the key management activities, preparation of debit / credit cryptograms, verification of debit / credit receipts etc.

To adhere to a set rule of quality and consistent specifications which is of prime importance in a project like NCMC, ISO, PCI certifications are a necessity. The smartcard used for NCMC project was finalised to be of ISO 14443 Type A and Type B specifications with open standards. This is an internationally used and acknowledged standard for the majority of smartcards in the transit industry world over. Specifications like this need to set to achieve seamless connectivity and integration. Example: Since the NCMC smart card is one of the core elements of the program, and the card forms the backbone of this system at the user level, the definition of the NCMC contactless smartcard is of prime significance.

After due deliberation and open bidding process, ISO 14443 Type A contactless smartcard has been selected to implement NCMC program for the first phase, the definition and specifications as defined in Appendix B were established based on the NCMC approach and methodology being discussed.

MoUD further circulated a NCMC concept note paper to all Public Transport Organisations and other stakeholders in all states of India on 19th October 2009, and posted the same document on its website. The document was prepared to give all interested parties an understanding of the proposed project, and receive constructive feedback and comments. These comments and suggestion were deliberated upon and incorporated in to the concept overview accordingly. Certain features of the NCMC were identified to be 'core' to its functioning, which included a clearing house, and AFC devices like ETM, Validators, ICU, PIS etc (Appendix C to F).

Lastly, developed standards and specifications were validated through the Global expression of interest. This has helped to get the consent of the leading industry experts who has vast experience and access to the state of art technology in the AFC domain.

Copyright © UTIITSL NCMC Project

6 OBSERVATIONS

Besides the various observations discussed above, certain focus areas were shortlisted for a successful implementation of a program like NCMC. Some simple but non-exhaustive observations are listed below:

(a) Fare / Ticket media integration and efficient clearance & settlement for distributed parties would be the hallmark of this project

(b) NCMC like systems already exist world over: Oyster Card of London, Octopus of Hong Kong, EZI Card of Singapore

(c) There are various transport projects worldwide with multiple chip vendors:

Europe (France, Scotland, Germany, Netherlands, Russia)

Asia (China, Singapore, Korea, New Zealand)

(d) Devices installed as a part of NCMC should ideally be PCI as well as EMV certified

(e) In a project like NCMC, ISO certifications are a necessity

(f) Constant need for evolution in processes and technology

(g) Requirement of a phased implementation of the NCMC.

(h) Focus that common, open national standards are adopted at all levels.

(i) Well defined system, process, equipment and interface specifications need to be issued by a central body to make the interoperability seamless and technically feasible.

7 INFERENCE

The procedure defined in this document helped achieve a systematic and efficient way to ascertain some salient features of the NCMC project, as well as point out some main focus areas that need to be addressed. An open national standard for achieving seamless connectivity and interoperability is a key issue which surfaced and is being addressed.

Copyright © UTIITSL NCMC Project

8 RESULT

Essential device and card minimum specifications

NCMC is an unprecedented national project of a large magnitude and importance. This project in its entirety will help enable and upgrade the business process and technological capabilities of various sectors of public transport, evolving the transportation industry to a new level.

The finalised minimum standard specifications for NCMC devices are provided in Appendixes A to F of this document and are as follows:

Appendix A	:	NCMC Security Access Module (SAM)
Appendix B	:	NCMC Contactless Smart Card
Appendix C	:	Electronic Ticketing Machine (ETM)
Appendix D	:	On-Board Validator
Appendix E	:	Integrated Control Unit (ICU)
Appendix F	:	Passenger Information System (PIS)

Copyright © UTIITSL NCMC Project

9 APPENDIX A: NCMC SECURITY ACCESS MODULE (SAM)

The SAM primarily combines with contact less smart card technology to provide security to device and transactions in multi-operator Automated Fare Collection Solution for the Public Transport in multimodal Transaction Clearing House environment which communicates at frequency – 13.56 MHz as per ISO 14443/2 & ISO 10373-6 to provide security support through a single SAM module. The SAM should have following minimum specification:

(i) Physical:- Mini-Sim type of SAM with 25mm length, width 15mm, thickness 0.76mm

(ii) Each SAM should have unique identification ID / number

(iii) Each SAM will have an internal memory of at least 32 K

(iv) Fast Contactless Transmission – Supports contactless smart cards up to 848 Kbps in fastest ISO 14443 A/B/ Sony Felica mode

(v) Designed for User Convenience – Housing design is optimized for advanced contactless applications

(vi) Mutual authentication with session key generation

(vii) Secure messaging

(viii) Protection against hardware attacks: Internal protections against SPA/DPA, direct memory scan and voltage variation

(ix) Flexible key diversification options,

(x) Secure download, storage

(xi) Data retention – 10 years

(xii) Compatibility with TimeCos, Sony Felica, Desfire, ISO standards etc.

Copyright © UTIITSL NCMC Project

(xiii) Supports:

(a) Cryptography and integrate:

- symmetric cryptography based on Triple DES and AES Encryption Algorithm
- asymmetric cryptographic for PKI based on RSA

(b) Protocols:- T=0 and /or T=1,

(c) Standard NCMC e-purse transaction time is controlled within 100ms

(d) Anti-plug-in, anti-pull-out and power off to protect data

(e) Anti collision

(f) Prevent data integrity loss

(xiv) Environmental conditional parameters (storage and operation):

(a) heat tolerance – -20 degree C to +85 degree C (at both operating condition & storage condition)

(b) humidity range – 15% to 95% (at operating condition)

& 15% to 100% (at storage condition)

(xv) Compliance with standards

(a) ISO/IEC 7810, ID-000

(b) ISO/IEC 7816 Part 1-4

(xvi) Supply, install, configure and commission required hardware and software to initialize and activate SAM.

(xvii) The SAM shall work with various NCMC compliant contactless smart cards manufactured by different card manufacturers.

Copyright © UTIITSL NCMC Project

10 APPENDIX B: NCMC CONTACTLESS SMART CARD

The Impact of the card selection goes a long way in the successful implementation of the NCMC project. Some of the considerations are as follows:

(a) To be suitable, the data modeling has to be broad enough to be used on a national basis.

(b) Non-standard cards (i.e. not ISO 14443) will not be supported to avoid any severe hardware impact

(c) Only Microprocessor based contactless cards will be supported to have a stable, scalable and highly secure tamper proof system.

Thus, a contactless ISO 14443 Type A microprocessor card has been selected for the NCMC project.

Since the card is a microprocessor based card, it has a flexibility of managing the data in an organized file structure.

A detailed specification document has been provided in this section (Appendix B) consisting of

(a) Technical Specification (Physical & Electrical Characteristics)

(b) NCMC Card Data Layout and Transaction flow.

Apart from transit application, the card will also be set up to add following facilities in addition to transit.

- Passes and other fare products
- Utility Payments
- Retail purchase related payments
- Toll Payments
- Parking etc.

Key Management information is given under section NCMC Security Model.

10.1 Technical Specifications:

Item	Description
1. Physical Characteristics	
a) Card Geometry	Shape and Physical Dimensions (including thickness) to be compliant to ISO 14443-1 standard

b) Base material	The complete base material including card body and transparent outer layer should be high grade PET-G. The surface must be such that it is low sensitive to dust and moisture adherence.
c) Card lifetime	Card lifetime must be more than 5 years. Therefore during this lifetime, the card must not develop cracks, hole, printing fading, major surface imperfection etc., due to aging.
d) General characteristics	Card must adhere to specifications covered in ISO IEC 10373-1 General characteristics (for following parameters): (a) Resistance to dynamic bending stress (b) Torsion stress (c) Bending stiffness (d) Resistance to break (e) Flammability, Peel strength (f) Card war-page (g) Resistance to chemicals (h) Adhesion (i) Card stability etc. (j) any other applicable parameter
2. Electrical, Memory and Electronic Characteristics	
a) Distance of work	The card should work up to a maximum distance of 10 cms between the card and the reader. The card operation at 10 cms with minimum field strength of 1.5 A/m (according to ISO14443-2) should be tested as per ISO 10373-6 Test PCD
b) Baud Rate	106Kbps (mandatory), up to 848 Kbps or higher (optional)
c) Memory Size	Size – 4Kbytes minimum, higher accepted Structure – Flexible File
d) Interface frequency	13.56 Mega Hertz
e) Transport Protocol	ISO 14443-4, for full featured application
f) Crypto function Supported	3Key Triple DES (24 byte key)

Copyright © UTIITSL NCMC Project

g) Command Set	Dependent on the Smart Card platform. ISO 7816-4 commands for simple data manipulation and additional commands that will be shared in confidence for integration purpose would be ‘’accepted’’ in order to achieve faster transactions and transaction integrity.
3. Other Essential Characteristics	
a) Read / Write endurance	100,000 cycles
b) Data Retention	10 years
c) Card Antenna	The Construction of the Card Antenna - Conventional copper based antennae is the preferred technology for the NCMC card. However the antennae should be embedded type only for long durability and better readability.
4. Certifications	
	(i) The card should comply with all standards / specifications covered under ISO 14443 Type A standard for contactless smart cards. (ii) The card conforms to the following essential electrical parameters, protocols and characteristics of Type A and B contactless RF Card Chip. Such parameters (but not limited to) include: a) Antenna coil size, b) Card chip / antenna inlay design c) Communication frequency d) Operating field strength, Modulation e) Read/Write Time, Data transfer rate f) Security features such as Anti-tearing, Momentary power loss protection, Anti-collision, Data integrity (support mutual authentication with the reader), Triple-DES encryption, EEPROM failure automatic detection, Transaction atomicity.
5. Security Features	

a) Card Tamper Protection	Card opening must not be possible without breaking the card itself and card must become useless. If card is opened, it should become unusable.
b) Hardware Security Certification	CC EAL 4+ for Hardware
6. Environmental condition parameters	
a) Resistance to environment	Cards must resist up to environment stresses as: Temperature: +60°C Relative Humidity: 100 %
b) Storage condition	Temperature: - 25°C to + 85° C Relative Humidity: 15 to 100 %
c) Operating condition	Temperature: - 25°C to + 85° C Relative Humidity: 15 to 100 %

10.2 NCMC Card Data Layout and Transaction flow:

This emphasizes the importance of having a common standardized card layout. Along with the standardized Card Layout, it's of utmost importance to have a standardized practice for Key Management. The keys to be managed will be divided into broadly three categories:

- Common Mobility Purse Keys (Issuer Keys)
- Non-Common Mobility Purse Keys (Non-Issuer Keys)
- Other Data (Active Fare, Personalization and non-Transit usage) Keys.

As can be seen, the Keys for Common Mobility Purse application and its files will be owned and managed by the National Transaction Settlement House.

The NCMC Card Data Layout and Transaction flow specification will provide the information necessary for NCMCs to be implemented and used.

10.2.1 Abbreviation

Definition	Description
3DES-CBC	3Key Triple DES operation in CBC mode
3DES-ECB	3Key Triple DES operation in ECB mode
CAN	Card Application Number
Card Rand	8 byte random number generated by the card
NCMC	National Common Mobility Card
CK2f	SFI of the EF containing the Credit Key #2

Copyright © UTIITSL NCMC Project

CK2n	Credit Key no 2 to be used by card in Credit transaction
CSN	Chip Serial Number
ADF	Application Directory file
EF	Elementary File
IV	Initialization vector to be used in Triple DES CBC operation
Pf	Purse File SFI
PTC	Purse Transaction Counter
Term-Date & Time	4-byte Date and Time value (in seconds) provided by the terminal
Term-Rand	8-byte random number generated by the terminal
TRP	Terminal Reference Parameter
SKf	SFI of the signature key file
SKn	Signing key number to be used by the card

10.2.2 Scope Objective

This section shall serve as a handbook for implementing National Common Mobility Card application or any terminal application which shall communicate with it. The section shall describe the file structure required for NCMC, its security architecture and all supported command interfaces.

All the specified command sets in this specification are independent of the underlying protocol. However, these command sets are greatly dependent on the file structure.

10.2.3 General Description

NCMC targets to provide a simple yet effective and secured e-Purse application for all kinds of transportation needs. This e-Purse can hold various transit fare products as well as various merchandize products. It has been designed to be a purely multi issuer – multi acquirer application, giving total freedom to its issuers as well as end users.

The highlighted features of this application are:

- It's a multi issuer – multi acquirer application where post issuance addition of acquirers is possible. Each of these acquirers can have their own key or even their own key file.
- A separate transaction log file has been maintained which keeps track of the recent transactions. The log of each transaction shall be recorded as a part of transaction without requiring any extra command.
- As "Credit" being most sensitive command, so it has been protected by 3 pass authentication. Three different 3DES keys can be used in a single credit operation, although it's not necessary that these three keys should have to be different.
- Debit operations are protected by 2 pass authentication using two different 3-DES keys.

Copyright © UTIITSL NCMC Project

- The Debit operation supports a special feature named Auto-Top-up. This ensures an un-interrupted service to the end user. Auto-Top-up happens with a pre specified amount to the Purse balance if the latter goes below a certain limit fixed by the Issuer. This operation can be traced back by the transaction log and later the amount can be settled with the acquirer.
- The Debit command can also be used for refunding a partial amount. However, the amount to be refunded must be less than the previous Debit amount. This feature is typically useful for all transit environment where in the total cost of the journey can be deducted from the purse at the beginning and later based on the distance travelled a certain amount can be refunded back.
- Atomicity for this application has been expanded to support multiple commands. Which means one Credit or Debit operation and update operation on a few other NCMC or non-NCMC files can be done atomically. The number of additional files which can be included in a single atomic operation is only limited by the size of atomic buffer created during personalization.

10.2.4 Functional Description

This part describes the functional requirements of NCMC.

10.2.4.1 File Structure

The NCMC mandates the presence of a particular file system, however doesn't mandate the creation of it. The NCMC ADF should be created under MF and this ADF shall contain all other NCMC related files such as Purse EF, Key EFs, Transaction log EF etc.

To enhance the transaction time it is mandatory that the NCMC ADF should be default selected after reset so that any other NCMC commands can be processed by the card without issuing any explicit select application command. Furthermore to enhance the interoperability among various implementations few File Identifiers and Short File Identifiers have been fixed by this specification.

Typically a NCMC compliant card must have a file structure as depicted in figure below.

Copyright © UTIITSL NCMC Project

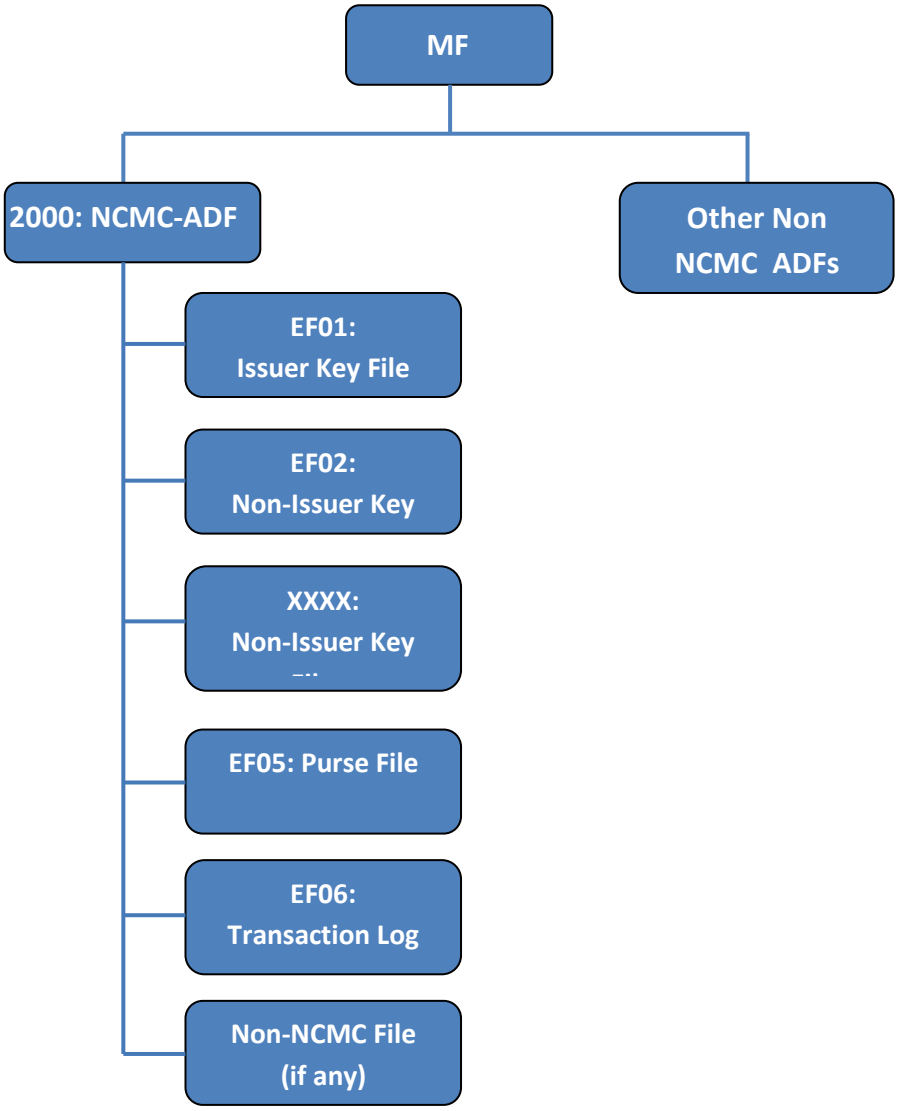

Figure 1: Typical NCMC file structure

There can be only one Purse EF and Issuer Key EF per NCMC ADF. However, the number of Non-Issuer key EFs is only limited by the allowed number of EFs in a DF. The purpose of differentiating the key EFs in to two different types is to limit the usage of the Keys. The keys stored in Issuer Key EF are authorized to do certain operations which are not permitted for the keys in Non-Issuer key EFs. Each acquirer of the application can have his own Non-issuer key EF if required and by this they can control their own keys separately.

Copyright © UTIITSL NCMC Project

10.2.4.1.1 NCMC ADF

The NCMC ADF shall be created under MF and shall be referenced by its file ID. Optionally it can also be referred by its AID. To perform a NCMC transaction this ADF must be selected first. Any NCMC command without selecting this ADF shall result in an error.

10.2.4.1.2 Issuer Key File

In a NCMC ADF there can be only one Issuer Key File. This EF shall contain all the Issuer keys. An Issue key EF shall be identified by the presence of its SFI in the Purse EF.

Item	Value	Remark
File ID	0xEF01	This is a mandatory value
SFI	0x01	This is a mandatory value
Access Condition	Proprietary	Although proprietary, following conditions should be met: Read: Never Update: Never
File Type	Binary	This is a mandatory
Size	2 + (25 * No of keys)	-

10.2.4.1.2.1 Data Format:

Byte 1	Lock/Unlock Byte	
Byte 2	Total No. of Keys in file	
Byte 3 ~ 28	Key Type 1	Key 1
Byte 29 ~ 54	Key Type 2	Key 2
:	:	
Byte N ~ N+25	Key Type n	Key n

a) Lock/Unlock Byte

This byte indicates if keys in the key file can be updated or not. If this byte is 0xFF, the keys can be changed using the Atomic Update command. If it is other values, the key file will be locked and no further updates of keys are allowed. This byte will be a write-once only byte i.e. once this byte had been modified, no further changed will be allowed.

b) Total No. of Keys in file

This byte indicates the number of set of keys available in the file.

c) Set of Keys

Each set of keys will be of 25-bytes in length and consist of 24-bytes key value and 1-byte key type.

Key Type	Key Value
1 byte	24 bytes

The format and the meaning of Key Type field:

Bit 8 – 5	Bit 4	Bit 3	Bit 2	Bit 1
RFU	Debit with Auto-Top-up Attribute	Signature Attribute	Debit Attribute	Credit Attribute

Attribute = 0 – not allowed

= 1 – allowed

10.2.4.1.3 Non-Issuer Key File

Multiple Non-Issuer Key file can exist within a NCMC ADF. Each acquirer can have one of these files for storing its keys or also can share the same EF.

Item	Value	Remark
File ID	XXXX	Can be any value which doesn't conflict with existing ones.
SFI	XX	Can be any value which doesn't conflict with existing ones.
Access Condition	Proprietary	Although proprietary following conditions should be met: Read: Never Update: Never
File Type	Binary or Record	Depends on implementation
Size	25 * No of keys	-

The data format of this EF is also the same as Issuer key EF.

10.2.4.1.4 Purse EF

This is the most important EF. In each NCMC ADF there can be only one such EF.

Item	Value	Remark
File ID	0xEF05	This is a mandatory value
SFI	0x05	This is a mandatory value

Copyright © UTIITSL NCMC Project

Access Condition	Proprietary	Although proprietary following conditions should be met: Read: Never Update: Never
File Type	Binary	This is a mandatory.

The data part of Purse EF should be organized as shown in the table below.

Field Name	Size
NCMC Version	1
Purse Operational Status	1
Maximum Purse Limit	3
Purse Balance	3
Auto-Top-up Amount	3
Auto-Top-up Interval (in days)	1
Valid Issuer Key File SFI	1
Valid Transaction Log File SFI	1
Purse Modify Transaction Type	1
Purse Configuration Byte	1
Last Credit Transaction TRP	4
Last Credit Transaction Header	8
Last Transaction TRP	4
Last Transaction Signed Certificate	8
Last Transaction Debit Options Byte	1
Purse Transaction Counter	3
Add Value Counter	3
Modify Purse Counter	2
Purse Expiry Date (Julian Date)	2
Purse Creation Date (Julian Date)	2
Date of Last Auto-Top-up operation	2
Card Application Number (CAN)	8
Card Serial Number (CSN)	8
Length of Issuer Specific Data	1

Copyright © UTIITSL NCMC Project

Issuer Specific Data	255

1) NCMC Version

- This byte is provided by the issuers during personalization. Current value of this field should be 0x01.

2) Purse Operational Status

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
RFU	RFU	RFU	RFU	RFU	RFU	Auto-Top-up Enabled	Purse Enabled

Auto-Top-up Enabled:

= 0: Auto-Top-up feature is disabled

= 1: Auto-Top-up feature is enabled

Purse Enabled:

= 0: purse operation is disabled

= 1: purse operation is enabled

- It indicates the current operational features that are enabled on the card e.g. Purse enabled, Auto-Top-up enabled etc.
- If the bit is set, the feature is enabled, otherwise it is disabled.
- Card OS will check this byte during debit or credit command to see if Auto-Top-up or purse operation can be allowed.

3) Maximum Purse Limit

- This stores the maximum purse value that can be supported by the purse.
- The Card OS shall have to check this value during Credit transaction to ensure that the Purse balance doesn't go beyond this limit. And if it is so then the Credit command shall be rejected by the card.

4) Purse Balance

- It is a 3-byte signed integer value.
- It indicates the purse value. For example, value 200 (in decimal) means Rupees 2.00.

5) Auto-Top-up *Amount*

- It specifies the amount to be added to the purse balance value when Auto-Top-up feature is triggered.

6) Auto-Top-up *Interval*

Copyright © UTIITSL NCMC Project

- It specifies the minimum interval in days from the last Auto-Top-up transaction that had to pass before the next Auto-Top-up transaction can be performed.

7) Valid Issuer Key File SFI

- This byte shall indicate the SFI of the Key File which shall be treated as the Issuer key file. Only the Keys residing under this Issuer Key file can be used for Credit operations.

8) Valid Transaction Log File SFI

- This byte indicates the valid Log File SFI that is to be tied to this purse. This log file shall then be updated upon successful transaction.

9) Purse Modify Transaction Type

- This byte indicates the valid transaction type that is to be used in order to perform a purse modification operation.
- Only Credit Command with this transaction type is allowed while issuing Debit Command with this transaction type shall result in an error.

10) Purse Configuration Byte

- Byte format:

Bit 7-Bit 2	**Bit 1**	**Bit 0**
RFU	Partial Refund Check	Issuer Key Check

Issuer Key Check:

Issuer can use this bit to restrict the usage of Non-Issuer Keys in Purse Debit operation.

= 0: Keys residing under any Non-Issuer key EF can be used for Debit operation.

= 1: Keys residing under Non-Issuer Key EFs can't be used for Debit operation.

However, this bit has no effect on the Credit operation as Credit operations are only allowed using keys residing under Issuer Key EF.

Partial Refund Check:

= 0: partial refund allowed

= 1: partial refund not allowed

- The partial refund parameter is needed to identify if the card shall allow performing partial refund. If the parameter indicates that it is not allowed, the card shall not allow partial refund to be processed and the transaction shall be denied.

11) *Last* Credit Transaction TRP

- It stores the TRP of the last credit transaction.

Copyright © UTIITSL NCMC Project

- Card OS will update this for each successful credit transaction. However, this field shall not be updated for Purse Modify Command.

12) *Last Credit Transaction Header*

- It stores the transaction header of the last credit transaction.
- Card OS will update this for each successful credit transaction. However, this field shall not be updated for Purse Modify Command.

13) *Last Transaction TRP*

- It stores the TRP of the last transaction being performed.
- Card OS will update this for each successful transaction including Purse Modify Command.

14) *Last Transaction Signed Certificate*

- It stores the computed signed certificate of the last transaction being performed.
- Card OS will update it for each successful transaction including Purse Modify Command.

15) *Last Transaction Debit Options Byte*

- It store the Debit Options Byte used by last debit transaction.
- This field is not updated for a credit transaction.

16) *Purse Transaction Counter*

- It indicates the number of transactions that actually occurred on this purse.
- Card OS will increment it by one each time there is a successful transaction, following the rule as described in section Counters and Usage.
- When the maximum value is reached, the purse will be disabled and no further transaction is allowed.

17) *Add Value Counter*

- It indicates the number of times that an add-value transaction occurred on this purse.
- Card OS will increment this value by one, each time a top-up transaction occurs, following the rule as described in section Counters and Usage.
- The Auto-Top-up transaction shall also be considered as a top-up transaction.
- A partial refund transaction will have no effect on this counter.
- When the maximum value is reached, the purse shall be disabled and no further transaction is allowed.

18) *Modify Purse Counter*

- It indicates the number of times that the Purse Modify Command has been performed on this purse successfully.

Copyright © UTIITSL NCMC Project

- Card OS will increase this value by one each time the Purse Modify Command is done, following the rule as described in section Counters and Usage.
- When the maximum value is reached, the purse will be disabled and no further transaction is allowed.

19) Purse Expiry Date

- This stores 2-byte expiry date of the purse using Julian Date format, expressed in days from a reference value defined by the issuer or interoperable scheme.
- Card OS shall check the current transaction date-time against these to determine the validity of the application. And if not valid then card OS shall reject the command.

20) Purse Creation Date

- This stores 2-byte creation date of the purse using Julian Date format, expressed in days from a reference value defined by the issuer or interoperable scheme.
- Checking of this value is not necessary during a transaction.

21) Date of Last Auto-Top-up operation

- It indicates the date of the last Auto-Top-up operation being performed on this purse.
- It is a 2-byte date in Julian Date format, expressed in days from a reference value defined by the issuer or interoperable scheme.

22) Card Application Number (CAN)

- These bytes are provided by the purse issuer during personalization and can be used for identifying the Issuer. The application doesn't interpret these internally.

23) Card Serial Number (CSN)

- These 8 bytes can be used to identify a particular card and the value of these should be same as the chip serial number.

24) Length of Issuer Specific Data

- This byte indicates the length of the Issuer Specific Data that follows.

25) Issuer Specific Data

- It contains the data specific to the issuer. Card OS shall not interpret this.
- 255 bytes have been reserved for this.

10.2.4.1.5 Transaction Log File

This EF shall be used for maintaining Transaction Logs and shall be updated internally after every NCMC transaction.

Item	Value	Remark

File ID	0xEF06	This is a mandatory value
SFI	0x06	This is a mandatory value
Access Condition	Proprietary	Although proprietary following conditions should be met: Read: Never Update: Never
File Type	Cyclic Record file	This is a mandatory.
Size	16 * No of records	-

10.2.4.1.6 Non-NCMC Files

Any number of Non-NCMC files can be created inside the NCMC ADF until the created EF doesn't conflict with any of the existing NCMC EFs. The header of theses EFs can optionally contain 2-extra bytes. One of these bytes shall refer to the Key EF SFI and the other shall refer to a key no. While using Atomic Update command to update such an EF the key used to derive the Atomic Update session key must match this key reference.

10.2.5 Security Architecture

The NCMC specification doesn't mandate any particular security architecture however, mandates the security aspects of each EF as mentioned in the File Structure section.

10.2.6 Counters and Usage

There are 3 counters which are used in NCMC transactions. Such as Purse Transaction Counter, Add Value Counter and Modify Purse Counter.

10.2.6.1 Purse Transaction Counter

Purse Transaction Counter (PTC) is a 3-byte value associated with the Purse EF. This counter shall be incremented each time a Debit or Credit operation happens. This counter shall be used to produce the "Signed Transaction Certificate" and as this counter is incremented every time so even if all other parameters are same the calculated certificate would be different each time. When this counter reaches the maximum value (2^{24} - 1) the NCMC application shall not accept any further Debit or Credit command and the PTC shall remain at its maximum value.

10.2.6.2 Add Value Counter

This is a 3-byte counter value maintained by the NCMC application. This counter shall keep track of the purse top-up transactions (Credit, Auto-top-up etc.). When this reaches its maximum value the application shall reject any further top-up transaction.

10.2.6.3 Modify Purse Counter

This is a 3-byte counter value which used to keep track of the Purse Data modification transactions. Each time any purse related data has been modified this counter shall be

Copyright © UTIITSL NCMC Project

incremented by 1 and when this reaches its maximum value the application shall reject all other Purse Modify related commands.

Following table shows the rules for incrementing each of the above mentioned counters:

Counter Data Increment Rules				
Description	**NCMC command**	**Counter Data**		
		PTC	**Add-Value counter**	**Modify purse counter**
Debit purse commands	Debit	√		
Debit purse commands with Auto-Top-up	Debit	√	√	
Purse disable command	Debit	√		
Auto-Top-up disable command	Debit	√		
Credit purse commands	Credit	√	√	
Modify purse data/Status command	Credit	√		√

10.2.7 Key types and its usage

NCMC application supports 4 different types of keys. All these keys must be 24-bytes in length.

10.2.7.1 Credit Key

These keys are present inside the Issuer Key EF and shall be identified by the Key Type. All the Credit operations must be performed using this key, however few Debit operations also requires the use of these keys.

10.2.7.2 Debit Key

These keys can be present in both Issuer and Non-Issuer Key EFs and shall be identified by its key type. Debit keys can't be used for Credit operation.

10.2.7.3 Auto-Top-up Key

These keys can be present under any of Issuer or Non-Issuer key EFs and shall be identified by it key type. When Debit with Auto-Top-up option is used in Debit transaction command the key used must have this attribute. Otherwise the card shall return an error. Auto-Top-up keys can't be used for Credit operations.

10.2.7.4 Signing Key

These keys can be present under any of Issuer or Non-Issuer key EFs and shall be identified by its key type attribute. Signing keys can't be used for Credit operations.

Operation Type	Key Usage			
	Credit Key	Debit Key	Auto-Top-up Key	Signing Key
Read Purse (with authentication)		√	√	√
Debit – Purchase (including partial refund and cumulative debits)		√	√	√
Debit – Purchase with Auto-Top-up			√	
Debit – Purse disable		√*	√*	√*
Debit – Auto-Top-up disable		√*	√*	√*
Credit Purse	√			
Credit – Modify purse data/Status	√			
Signed certificate generation	√	√	√	√

Note: * Depending on Purse Configuration, these keys may be required to reside in the Issuer Key File

10.2.8 Command Description

Following table shows the basic commands which are to be supported by NCMC application. Apart from these the card can also support the personalization related commands, however, those commands should not be active during usage phase.

No.	Commands	CLA	INS	Type
1	Get Data	00	CA	Administrative
2	Credit Purse	90	36	NCMC v1.0
3	Debit Purse	90	34	

Copyright © UTIITSL NCMC Project

4	Read Purse	90	32	
5	Atomic Update	90/91	40	
6	Get Challenge	00	84	

10.2.8.1 Get Data

This command can be used to read the card information i.e. card ATR and historical bytes.

10.2.8.1.1 Condition:

- This command can be used during both personalization and normal operation.

10.2.8.1.2 Command Format:

Parameter	Value
CLA	0x00
INS	0xCA
P1	See Below
P2	See Below
Lc	-
Data	-
Le	0x08 / 0x00

10.2.8.1.3 Data Response:

P1P2	Meaning
0x5F51	Contact ATR information.
0x5F52	Chip serial number (8 bytes)

10.2.8.1.4 Response Status word:

SW1 SW2	Description
9000	Command executed successful
6700	Wrong Le
6A86	Wrong parameter P1, P2
6E00	Wrong CLA

10.2.8.2 Read Purse

This command is used to read purse information as well as to retrieve the purse transaction log data. This is generally the first command in any transaction. The

Copyright © UTIITSL NCMC Project

response data to this command shall contain the CAN and CSN which shall be used in derivation of session keys for further card usage.

10.2.8.2.1 Condition:

- For Read Purse secure a Get Challenge command must precede it.
- Read Purse secure can only be allowed with Debit, Auto-Top-up or Signature key types.

10.2.8.2.2 Command Format:

Parameter	Value
CLA	0x90
INS	0x32
P1	Purse File SFI
P2	0x00
Lc	0x00 / 0x01 / 0x0A
Data	See below
Le	Length of data to read

10.2.8.2.2.1 Data Sent:

Lc = 0:

No data is sent. This mode is used to read the Purse File without any security.

Lc=1:

This mode is used to read the transaction log records.

Record Offset
1-byte

The Record Offset shall specify the starting log to be read up to either the record specify in the Le or the end of records in the Log EF.

Lc=10:

This is used to perform a Read Purse Data with mutual authentication.

Debit, Auto-Top-up or Signature key		Terminal random number
Key file SFI	Key number	
1-byte	1-byte	8-bytes

10.2.8.2.2.2 Data Response:

Data Object	Length (Byte)	Security
CMC version	1	None
Purse Status	1	None
Purse Balance	3	None
Auto-Top-up amount	3	None
CAN	8	None
CSN	8	None
Purse expiry data (Julian Date)	2	None
Purse creation data (Julian Date)	2	None
Last credit transaction TRP	4	None
Last credit transaction header1	8	None
No. of records in transaction Log File	1	None
Issuer-specific data length	1	None
Last transaction TRP	4	None
Last transaction record	16	None
Issuer-specific data	X	None
Last transaction debit options byte	1	None
Last transaction signed certificate	8	Triple-DES CBC
Counter data	8	Triple-DES CBC
ISO/IEC 14443-3 CRC_B	2	None

The 'Last transaction signed certificate', 'Counter data' and 'ISO/IEC 14443-3 CRC-B' are only returned when a Read Purse Data with mutual authentication is performed. The Read Purse encrypted data consisting of 'Last transaction signed certificate' and 'Counter data' is computed as illustrated in Read Purse Encrypted Data Computation. The 'ISO/IEC 14443-3 CRC-B' is computed over the unencrypted 'Last transaction signed certificate' and 'Counter data'.

Copyright © UTIITSL NCMC Project

10.2.8.2.3 Read Purse Encrypted Data Computation

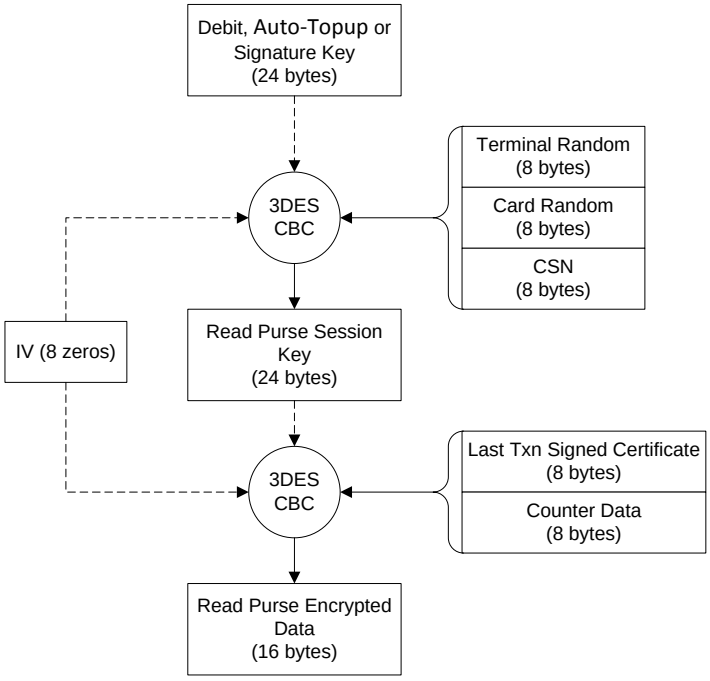

Figure 2: Read Purse Encrypted data computation

10.2.8.2.4 Response Status word:

SW1 SW2	Description
9000	Command executed successful
6700	Wrong Le, Lc
6985	Condition of use not satisfied
6A80	Wrong parameter in data field
6A82	File not found
6B00	Wrong parameter P1, P2
6E00	Wrong CLA

10.2.8.3 Credit Purse

This command is used to perform a credit transaction as well as modifying the data in the Purse EF. This command is designed to accept total three key references which can be the same keys or different. The Credit process starts off by the terminal sending an 8-byte terminal random number and a credit cryptogram packet. This random number in conjunction with card random number and Chip Serial Number shall be used to derive the credit session key. This session key shall be used to decrypt the Credit Cryptogram. After decryption of the Credit Cryptogram card shall verify the SKf, SKn, Credit record CRC and shall throw an error in case of any mismatch.

The Credit record CRC is an ISO/IEC 13239 CRC checksum calculated over the TRP, Pf, SKf, SKn and Transaction Log Record in that order.

Copyright © UTIITSL NCMC Project

Once card has finished all the necessary checking it shall update the Purse content (Amount or any other field as specified) and prepare a receipt cryptogram. Also it shall update the transaction log file with the recent transaction record. All these file update operation should happen atomically.

10.2.8.3.1 Condition:

- Credit amount must be positive.
- Get Challenge command must be performed prior to this command.
- The two Credit Keys used here are must be from the Issuer Key EF. However, the signature key can be from the Issuer Key EF or from any other Non-Issuer Key EF.

10.2.8.3.2 Command Format:

Parameter	Value
CLA	0x90
INS	0x36
P1	CK2f
P2	CK2Kn
Lc	0x25
Data	Credit Cryptogram
Le	0x18

10.2.8.3.2.1 Data Sent:

Pf	Credit Key # 1		Signing Key		Terminal Random	Credit Cryptogram	Txn User Data
	Key EF SFI	Key No	Key EF SFI	Key No			
1 byte	1 byte	1 byte	1 byte	1 byte	8 bytes	16 bytes	8 bytes

Credit Record						
TRP	Credit Parameter Block					Transaction Date & Time
	Credit Record CRC	SKf	SKn	Transaction Type	Transaction Amount	
4 bytes	2 bytes	1 byte	1 byte	1 byte	3 bytes	4 bytes
				Transaction Header		

Pf – Purse File SFI.

CK2f – SFI of Credit Key #2

CK2Kn – Key number of Credit Key # 2

SKf – SFI of Signature Key EF

SKn – Key number of Signature Key

TRP – Terminal reference parameter

The Credit Record CRC is an ISO/IEC 1444-3 CRC_B checksum calculated over the TRP, Pf, SKf, SKn and Transaction Log Record in that order.

Credit Cryptogram is the result of applying 3-DES CBC on a 16-byte Credit Record data structure using a 24-byte Credit Session Key.

The Credit Command can also be used to perform a Modify Purse Data/Status command when a Modify Purse Data/Status transaction type is used. In this case the 3-byte transaction amount is interpreted as follows:

Modify purse status set bit mask	Modify purse data offset	Modify purse data length
1-byte	1-byte	1-byte (0-8)

Modify Purse Data length – specifies the number of bytes from the start of the transaction user data to update a logical area within the purse EF at a byte offset location specified by *Modify Purse Data offset*.

Modify Purse Status Set Bit Mask – specifies the bit mask indicating the bits to be set to 1 in the purse status byte.

Modify Purse Data offset: - Specifies the logical offset for data element to be updated within the Purse EF.

Offset	Field	Byte
0x00	Total available Records in Log File	1
0x01	Maximum Purse Limit	3
0x04	Purse Expiry Date	2
0x06	Last Auto-Top-up Date	2
0x08	Auto-Top-up Interval	1
0x09	Auto-Top-up Amount	3
0x0C	Purse Configuration Byte (Extended Operational Status)	1
0x0D	Issuer Specific Data Length	1
> 0x0E	Issuer Specific Data	Variable

If the offset value used in command data is anything other than the above mentioned values then card shall reject the command with SW6A80.

Copyright © UTIITSL NCMC Project

When modifying a field, the total length of new data allowed is indicated as shown above for each field. E.g. offset 1 can only be updated up to 3 bytes. If exceed the mentioned size, the card shall return error 0x6A80.

The card does not allow modifying various fields together, i.e. modifying 'Issuer Specific Data Length' and 'Issuer Specific Data' in a single command. If it does, the card shall return error 0x6A80.

10.2.8.3.2.2 Command data preparation

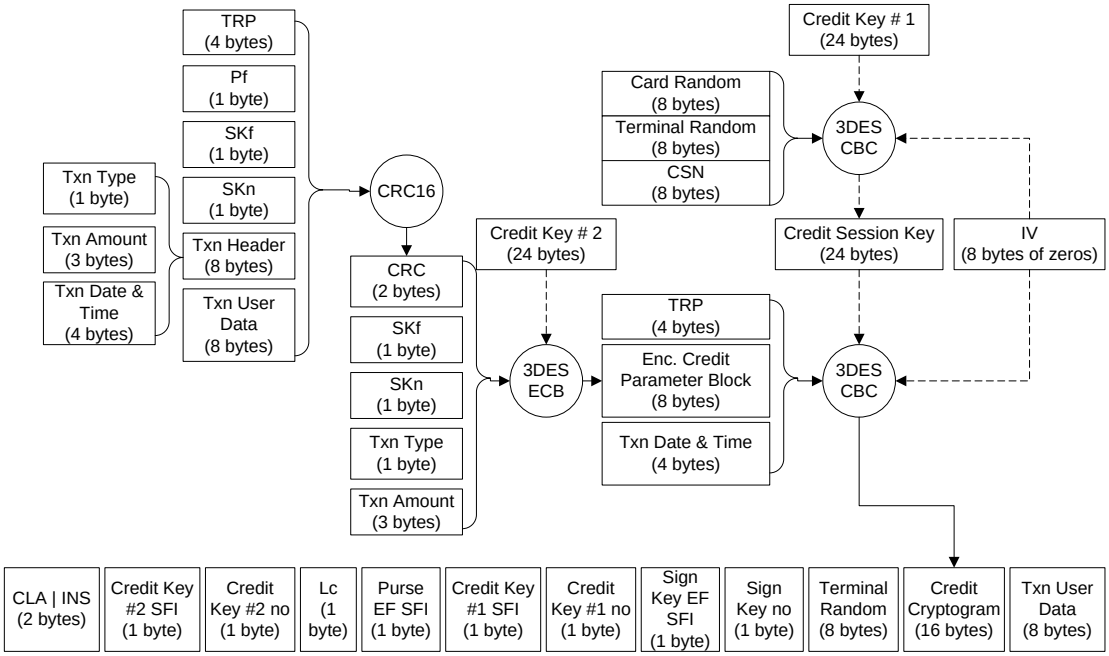

Figure 3: Credit Purse command data preparation

10.2.8.3.2.3 Data Response:

In response to Credit Purse command card shall reply with a Credit receipt cryptogram. The Credit Receipt Cryptogram is computed by doing a 3-DES CBC encryption (IV=Counter Data) of the 24-byte Credit Receipt Record using a 24-byte Credit Session Key. The computation of the Signed Certificate is depicted in section Computation of Signed Certificate.

Credit receipt record			
Purse balance	**Most significant 5-bytes of signed certificate**	**Signed certificate**	**Counter data**
3-bytes	5-bytes	8-bytes	8-bytes

10.2.8.3.3 Credit Receipt Cryptogram Computation

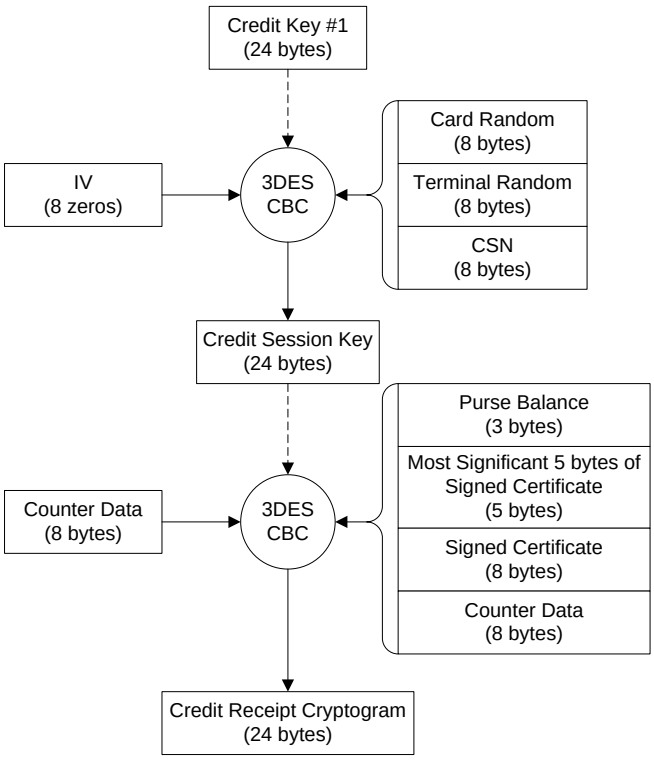

Figure 4: Credit Receipt Cryptogram Computation

10.2.8.3.4 Response Status word:

SW1 SW2	Description
9000	Command executed successful
6700	Wrong Le, Lc
6982	Security condition not satisfied CRC error
6984	Exceeded chaining buffer limit

Copyright © UTIITSL NCMC Project

6985	Conditions of use not satisfied Get Challenge not issued Card expired
6A80	Wrong parameter in data field Invalid modify offset or length
6A82	Purse File or Key File not found
6A84	Not enough memory space Counter value overflow
6B00	Wrong parameter P1, P2
6E00	Wrong CLA

10.2.8.4 Debit Purse

This command is used to perform a debit, debit with Auto-Top-up, partial refund and cumulative debit transaction. It has been designed in such a way that along with performing above it shall also read back the remaining balance amount and a transaction sign certificate. Similar to credit operation all file updates will happen atomically.

The process starts with terminal asking for a challenge from the card. Terminal shall send a terminal random number along with a debit cryptogram. Card shall make use of this terminal random, card challenge and CSN to derive the 24 byte debit session key. Using this session key card shall decrypt the debit cryptogram and verify the Debit record CRC, SKf and SKn. The debit record CRC is an ISO/IEC13239 CRC checksum calculated over the TRP, Debit option byte, Pf, SKf, SKn and the transaction log record in that order. Once all these checks are successfully done the card shall deduct the specified amount from the Purse Balance, write the transaction log record and update the relevant counters all as a part of single atomic operation.

10.2.8.4.1 Condition:

- Get Challenge command must be performed prior to this command.
- The transaction amount is a signed integer, where a negative value indicates a debit and a positive value indicates a credit (partial refund).
- Partial refund shall not be allowed if Purse Configuration byte doesn't support it.
- Debit with Auto-Top-up shall not be allowed if Purse Configuration byte doesn't support it.

10.2.8.4.2 Command Format

Parameter	Value
CLA	0x90
INS	0x34

P1	RFU
P2	Debit Option
Lc	0x25
Data Sent	Debit Cryptogram
Le	0x18

Response Data	Debit receipt cryptogram
Status Words	0x9000, 0x6982, 0x6A82, 0x6B00, 0x6985, 0x6A80, 0x6700

10.2.8.4.3 Debit Option Byte:

Debit Options							
B7	**B6**	**B5**	**B4**	**B3**	**B2**	**B1**	**B0**
1: Disable Expiry Checking	1: Auto-Top-up Disable	RFU	RFU	0: Deduct Purse 1: Deduct with partial refund 2: Cumulative Debit (Slicing) 3: Purse Disable 4..15: RFU			

10.2.8.4.4 Data Sent:

Pf	Debit Key		Signing Key		Terminal Random	Debit Cryptogram	Txn User Data
	Key EF SFI	Key No	Key EF SFI	Key No			
1 byte	1 byte	1 byte	1 byte	1 byte	8 bytes	16 bytes	8 bytes

Debit Record						
TRP	Debit Parameter Block					Transaction Date & Time
	Debit Record CRC	SKf	SKn	Transaction Type	Transaction Amount	
4 bytes	2 bytes	1 byte	1 byte	1 byte	3 bytes	4 bytes
				Transaction Header		

Figure 5: Debit command data

10.2.8.4.4.1 Command data preparation

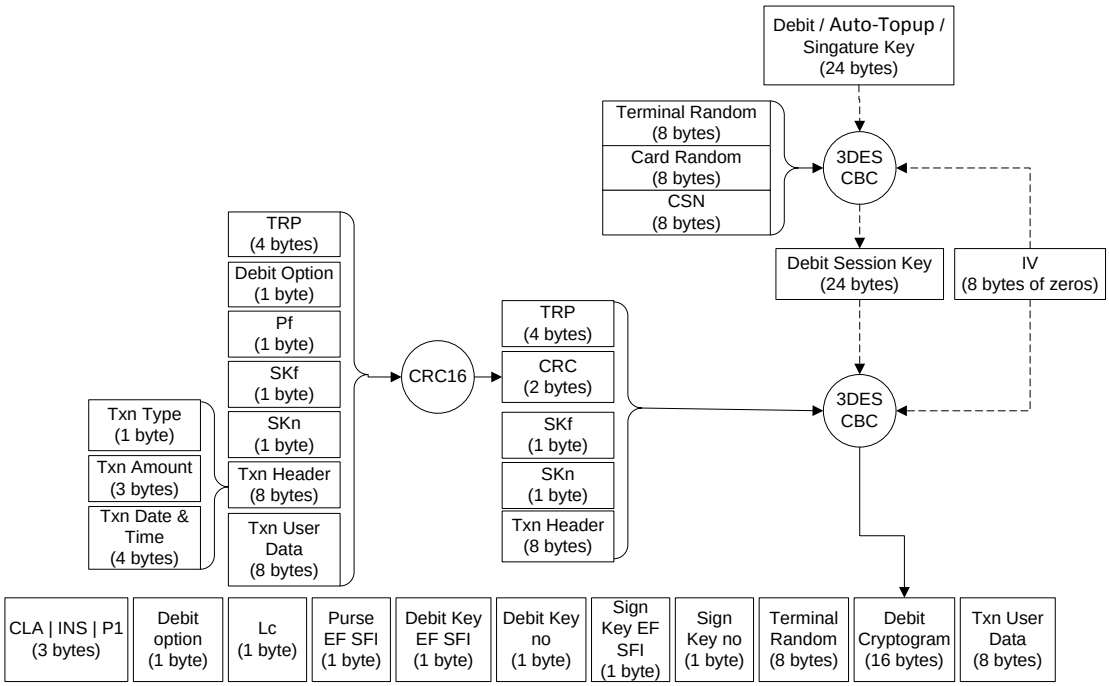

Figure 6: Debit command data preparation

10.2.8.4.5 Data Response:

In response to Debit command card shall return the Debit receipt cryptogram. The debit receipt cryptogram shall be calculated by performing a 3DES CBC encryption (IV = Counter Data) on the following debit Receipt Record by using the 24 byte Debit Session Key. The computation of Sign Certificate is described in section Computation of Signed Certificate.

Debit Receipt Record			
Purse Balance	**Most Significant 5 bytes**	**Signed Certificate**	**Counter data**

	of Signed Certificate		
3 bytes	5 bytes	8 bytes	8 bytes

10.2.8.4.6 Debit Receipt Cryptogram Computation

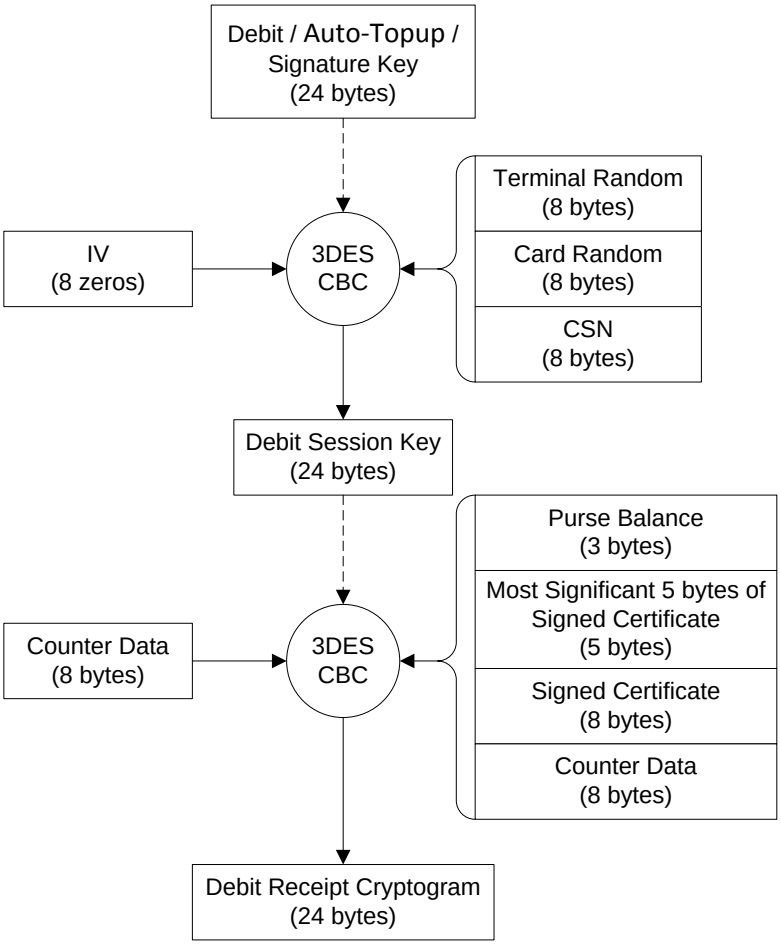

Figure 7: Debit Receipt Cryptogram Computation

10.2.8.4.7 Response Status word:

SW1 SW2	Description
9000	Command executed successful
6700	Wrong Le, Lc
6982	Security condition not satisfied CRC error
6984	Exceeded chaining buffer limit
6985	Conditions of use not satisfied Get Challenge not issued

Copyright © UTIITSL NCMC Project

	Card expired Use of Credit Key not allowed Not from Issuer Key File
6A80	Wrong parameter in data field
6A82	File not found
6A84	Not enough memory space Counter value overflow
6B00	Wrong parameter P1, P2
6E00	Wrong CLA

10.2.8.5 Atomic Update

This command is used to update certain number of EFs along with the Purse EF in a single atomic operation. A series of update command can be chained together using this command and all of those data shall be committed only after receiving the last command of the chain or a debit or credit command. Any interruption in between these commands in the form of power failure or error status shall break the chain and no data shall be updated.

10.2.8.5.1 Condition:

- This command can only be executed after a Read Purse command with authentication otherwise an error code is returned.
- If the command is not the last command in the atomic update chain then CLA=91 is used else CLA=90 is used.
- This command cannot be used to update Purse and Log EF.
- Updating of Key EF is allowed only if the file is not locked.
- This command can be performed independently or used together with a transaction command i.e. Debit or Credit. However, the transaction command must be the last command in the atomic chaining.
- Updating of an Application EF required that the Read Purse Secure session key used must belong to the Key SFI specified in the creation of this file during personalization.
- This command shall not be allowed if Signature Key is used during the Read Purse Secure. Only Debit and Debit with Auto-Top-up key type can be used to activate this command.

10.2.8.5.2 Command Format:

Parameter	Value
CLA	0x90 / 0x91
INS	0x40
P1	SFI
P2	Offset

Copyright © UTIITSL NCMC Project

Lc	Update Len + 4
Data Sent	Update Data + 4-byte MAC
Le	0x04

Response Data	4- LSB of MAC
Status Words	0x9000, 0x6982, 0x6A82, 0x6B00, 0x6985, 0x6A80, 0x6700, 0x6984

10.2.8.5.2.1 Data Sent:

Update Data String	MAC
Len bytes	4 bytes

The MAC sent is the 4 most significant bytes of ISO/IEC 9797 MAC. It shall be calculated over the data starting from the CLA to the last byte of the data to be updated (excluding MAC). The Lc used in calculation is the updated Lc which means it shall also include the length of MAC. The computation of MAC is depicted below.

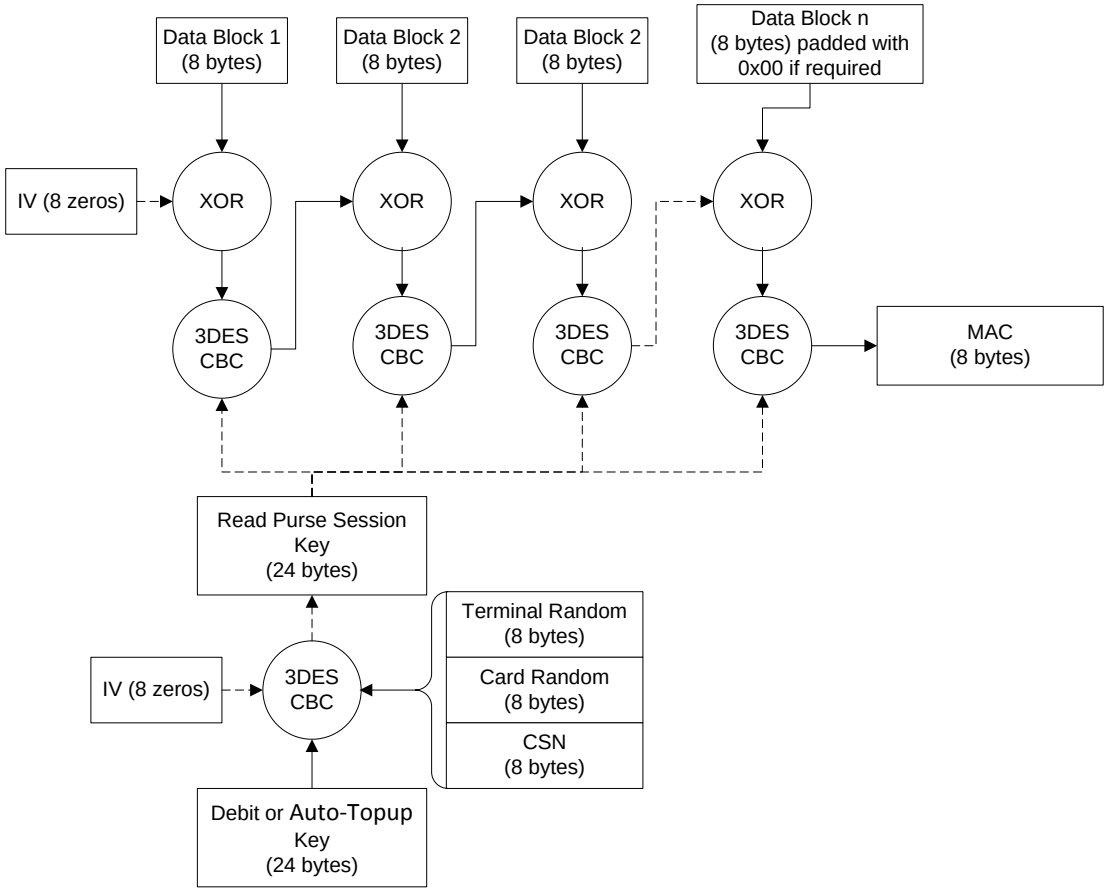

Figure 8: MAC computation

10.2.8.5.2.2 Data Response:

In response to Atomic Update command the card shall return the 4 LSB bytes of the MAC computed.

10.2.8.5.2.3 Response Status word:

SW1 SW2	Description
9000	Command executed successful
6700	Wrong Le, Lc
6982	Security conditions not satisfied Wrong MAC Updating key file not allowed Updating of Purse or Log EF not allowed
6984	Error in updating chaining buffer
6985	Conditions of use not satisfied No Read Purse Secure issued
6A82	File not found
6B00	Wrong parameter P1, P2 Wrong offset, exceed file size
6E00	Wrong CLA

10.2.9 Computation of Signed Certificate

Signed Certificate is a digital certificate which can be used as a proof of any particular transaction. This is computed by performing a Tripe-DES ECB encryption over the transaction header. Before computing the certificate, a signing session key is derived from the sign key whose reference has been provided in the Debit / Credit command data field. All counter data elements which are used in the derivation of the signing session key are incremented prior to use. The Debit Option byte shall be set to 0x00 in case of Credit command.

Copyright © UTIITSL NCMC Project

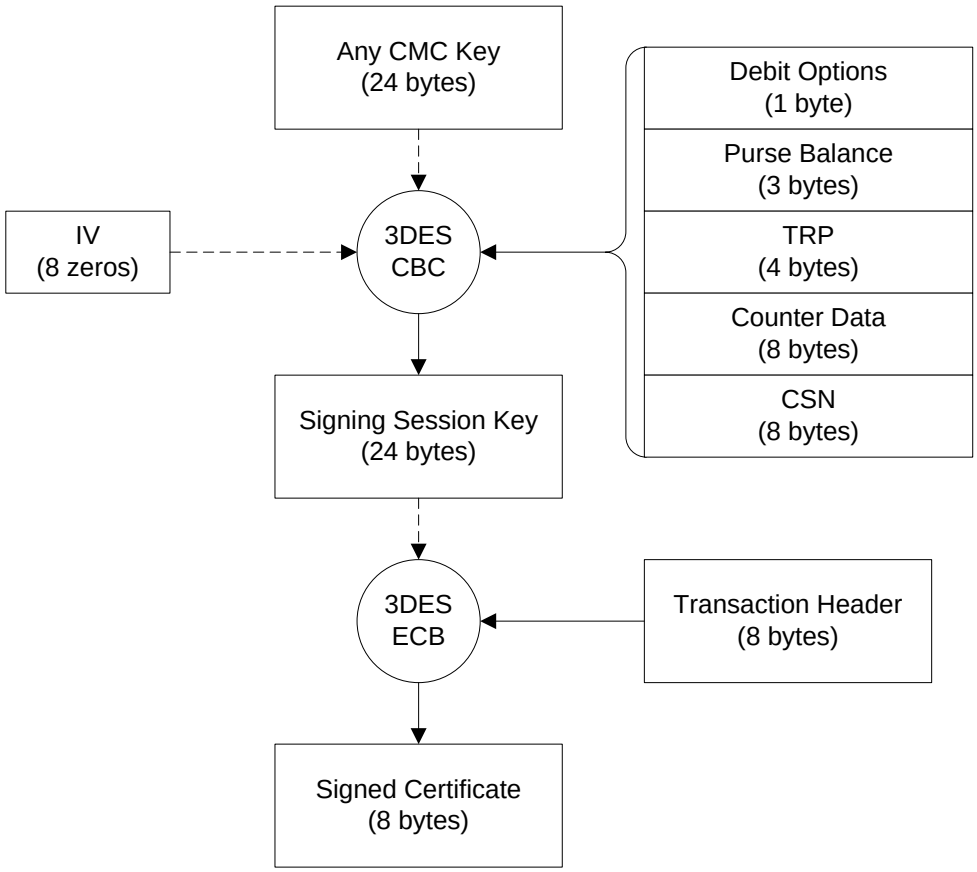

Figure 9: Computation of Signed Certificate

10.2.10 Data Element Dictionary

10.2.10.1 Card serial number

This is an 8-byte unique value generated by the chip. This can be used to uniquely identify a particular NCMC card irrespective of its issuer.

10.2.10.2 Card Application Number

This is an 8-byte number generated by the issuer which can be used to identify a particular NCMC card.

10.2.10.3 Balance and amount values

These are 3-byte signed values.

10.2.10.4 Date & Time

The 4-bytes Transaction Date & Time used in command data field are a big ending unsigned value expressed in seconds. And the 2-bytes Purse Creation Date and Purse Expiry Date fields are big-endian unsigned values expressed in days. The reference value for these values can be decided by the issuer. The values expressed in seconds can be converted into days by dividing by 86400.

Copyright © UTIITSL NCMC Project

10.2.10.5 Terminal Reference Parameter

This is 4-byte value used in transactions. The interpretations of these bytes are issuer specific and card shall not process these.

10.2.10.6 Transaction log

This is a buffer which can be implemented as an EF and shall contain the records of most recent transactions. The size of this EF can be decided during personalization. This should be implemented as a cyclic buffer where new records shall overwrite the oldest one.

10.2.11 Test Vectors

10.2.11.1 Signed Certificate

Sign Key	: B717600CB1EC11641E69372B4D9D0C11CA1ED1E5976314E6
Debit Option	: 00
Purse Balance	: 004D9E
TRP	: 11432400
Counter Data	: 0000010000010001
CSN	: A20D501F50033B1B
Sign Session Key	: 3DES-CBC (Sign Key) [Debit Options | Purse Balance | TRP | Counter Data | CSN]
	: EE12A396B1BF91EF3E1CA7C3F9B64CD46A32498DB0FE080E
Txn Header	: 30FFFF7E11432400
Signed Certificate	: 3DES-CBC (Sign Session Key) [Txn Header]
	: 04233035DA090040

10.2.11.2 Read Purse Response (With Authentication)

Read purse Key	: A554C7A956CBBCDE95E067FC9BE781907F52CD58DE3EB000
Card Rand	: B928702EF3F403C3
Terminal Rand	: 1234567887654321
CSN	: A20D501F50033B1B
Read Purse Session Key	: 3DES-CBC (Read Purse Key) [Terminal Rand | Card Rand | CSN]
	: E330A6250C25A63044883DC542C37B529CE6B78B53290D3D
Last Txn Signed Certificate	: 04233035DA090040
Counter Data	: 0000010000010001
Read Purse Encrypted Data	: 3DES-CBC (Read Purse Session Key) [Last Txn Signed Certificate | Counter Data]
	: 8C441457FB39CDABD94C30B6D781D8A9

Copyright © UTIITSL NCMC Project

10.2.11.3 Debit Cryptogram

TRP	: 11432400
Debit Option	: 00
Pf	: 05
SKf	: 01
SKn	: 03
Txn Header	: 30FFFF7E11432400
Txn User Data	: A80B5FD78D57BE00
Debit Record CRC	: CRC16 [TRP | Debit Options | Pf | SKf | SKn | Txn Header | Txn User Data]
	: 5215
Debit Key	: A554C7A956CBBCDE95E067FC9BE781907F52CD58DE3EB000
Card Rand	: B928702EF3F403C3
Terminal Rand	: 1234567887654321
CSN	: A20D501F50033B1B
Debit Session Key	: 3DES-CBC (Debit Key) [Terminal Rand | Card Rand | CSN]
	: E330A6250C25A63044883DC542C37B529CE6B78B53290D3D
Debit Cryptogram	: 3DES-CBC (Debit Session Key) [TRP |CRC |SKf | SKn | Txn Header]
	: 4DBD20EE129E63BA139D1A197FFB0F60

10.2.11.4 Debit Receipt Cryptogram

Debit Key	: A554C7A956CBBCDE95E067FC9BE781907F52CD58DE3EB000
Card Rand	: B928702EF3F403C3
Terminal Rand	: 1234567887654321
CSN	: A20D501F50033B1B
Debit Session Key	: 3DES-CBC (Debit Key) [Terminal Rand | Card Rand | CSN]
	: E330A6250C25A63044883DC542C37B529CE6B78B53290D3D
Purse Balance	: 004D9E
Signed Certificate	: 04233035DA090040
Counter Data	: 0000010000010001
Debit Receipt Crypt	: 3DES-CBC (Debit Session Key) [Purse Balance | 5 MSB of Signed Certificate | Signed Certificate | Counter Data]
	: 97B4919AF7C2C8E6649F0810EC1048364A8F2D035A02A415

Copyright © UTIITSL NCMC Project

10.2.11.5 Credit Cryptogram

TRP	: 11432400
Pf	: 05
SKf	: 01
SKn	: 03
Txn Header	: 750003E811432400
Txn User Data	: A80B5FD78D57BE00
Txn Date & Time	: 11432400
Credit Record CRC	: CRC16 [TRP | Pf | SKf | SKn | Txn Header | Txn User Data]
	: 377E
Encrypt Credit Parameter Block using Credit Key 2:	
Credit Key #2	: 0F30901ACC1432B6209A177F843C2606A99D16D3EBD2B0F4
Enc Credit Parameter Block: 3DES-CBC (Credit Key #2) [CRC | SKf| SKn | Txn Type | Txn Amount]	
	: 0CD5C266A516E098
Credit Key #1	: 12113D2CA4C3851617A03AD30D7152DC1916D25B21FA3788
Card Rand	: B928702EF3F403C3
Terminal Rand	: 1234567887654321
CSN	: A20D501F50033B1B
Credit Session Key	: 3DES-CBC (Credit Key) [Card Rand | Terminal Rand | CSN]
	: E7B3337BF0B93801891089B5816176CFD4432165D9094037
Credit Cryptogram	: 3DES-CBC (Credit Session Key) [TRP | Enc Credit Parameter Block | Txn Date & Time]
	: 016758F457F18F28898543CCA58AA491

10.2.11.6 Credit Receipt Cryptogram

Credit Key #1	: 12113D2CA4C3851617A03AD30D7152DC1916D25B21FA3788
Card Rand	: B928702EF3F403C3
Terminal Rand	: 1234567887654321
CSN	: A20D501F50033B1B
Credit Session Key	: 3DES-CBC (Credit Key) [Card Rand | Terminal Rand | CSN]
	: E7B3337BF0B93801891089B5816176CFD4432165D9094037
Purse Balance	: 018A88
Signed Certificate	: D28A4F3541AD7C82
Counter Data	: 0000010000020001
Credit Receipt Crypt	: 3DES-CBC (Credit Session Key) [Purse Balance | 5 MSB of Signed Certificate | Signed Certificate | Counter data]
	: EBF1D776BC179650ED972AD71CB4B0398308125DEE27B033

Copyright © UTIITSL NCMC Project

11 APPENDIX C: ELECTRONIC TICKETING MACHINE (ETM)

ETM Specifications	
Processor	Minimum 300 MHz Arm 7/ 9 / 11
Memory and Storage	
Flash	Minimum of 128 MB
RAM / SDRAM	Minimum of 32 MB upgradable to 64 MB
SD Card	Minimum 2 GB
Reader	
Card readers	Contactless Smart card as per ISO 14443 standards (Type A, Type B) and Sony Felica compliant
Magnetic card readers	Triple track (tracks 1,2,3), bi-directional
Input & Output	
Keypad	To have Programmable keys, Function keys and alpha numeric Keys. Minimum 15 keys with functional/navigation keys
Printer speed	Minimum 15 lines per second.
Thermal roll	Paper roll cage of minimum 25 mm to 40 mm
Display	Minimum monochrome graphical screen
Communication Interface	
Ethernet port	10/100/1000 Mbps
Serial Port	Minimum RS232
USB Port	Type A / Type B
Wireless	GPRS modem to suit Indian Frequency band/ Bluetooth GSM/GPRS on 850/900/1800/1900 MHz;
Security	
SAM Slots	Minimum of 2 and compliant to ISO standard 7816

Copyright © UTIITSL NCMC Project

EMV Certification (Mandatory)	Minimum EMV Certification Level 1& 2.
PCI / PED standards(Mandatory)	PCI PED 2.0 Certification
Cryptography Support with required certification	Triple DES for Key Management with UKPT (Unique Key Per Transaction)
CE / FCC or equivalent Certification	
Power and Charging	
Input power supply	Input 160 volt to 250 volt AC, 50 Hz
Battery	Minimum of 1800 mAh *With additional battery pack for long working period
Machine Charging	*Cradle charging and data download facility at Depot level *In-bus charging facility
Other	
Terminal Weight	Approximately 250 gm to 500 gm
Environmental compliance:	Operational temperature: -5°C to 45°C Operational humidity: 5% to 95%
*Online Support	Remote terminal Management and Software upgrade
*Software that can be run in parallel along with Fare collection software	Industry proven software application on the terminal
(Mandatory)	Electronic Ticketing Application
(Mandatory)	Credit / Debit Application
	Mobile Top up application
	Bill Pay application

Note: *Features and specification parameters are preferable for seamless operation.

12 APPENDIX D: ON_BOARD VALIDATOR

12.1 On-board Validator specification

(i) Card Reader Support:

(a) Support ISO 14443 Type A, Type B and Sony Felica
(b) Future capability to upgrade to: Near field Communication (NFC) devices, Credit/debit cards

(ii) Capacity:
(a) CPU: 400 Mhz processor
(b) RAM: Minimum 256 MB (should be upgradable to 2 GB)
(c) SRAM: minimum 256 KB (should be upgradable to 2 MB)
(d) Flash: Minimum 256 MB (Upgradable to 2 GB)
(e) Clock: Real time, battery backed.

(iii) Environment:
(a) Storage Temperature: -25 to 85 degree centigrade
(b) Operating Temperature: -20 to 60 degree centigrade
(c) Relative Humidity: 5% to 95%

(iv) Communications:
(a) 10/100/1000 Mbps Ethernet Port
(b) RS 232
(c) Minimum 2 SAM card slots, compliant to ISO 7816 standards
(d) USB ports (Type A / Type B)

(v) Patron interface:
(a) Multi-lingual support
(b) Digital audio/buzzer
(c) Bright colour TFT screen with capability to support high resolution graphics. Contrast and brightness adjustment facility. LED indications for status display
(d) Fully programmable user interface

(vi) Options:
(a) WLAN, GPS, 3G/GPRS
(b) Custom logos and artworks

(vii) Power supply: 10V - 48V DC

(viii) Hardware
(a) Housing specifications: Robust design, rugged and durable
(b) Hardware protection: Shock/vibration proof with requisite certifications if applicable
(c) Mechanical Stress: Vibration: 0.3g (rms), 5 to 200 Hz (on all axes), shock: 4g peak (duration 20 ms), inclination: remain operative up to 10° off vertical , un-sustained

(ix) Compliance:
(a) EMV Certification minimum Level 1
(b) CE / FCC or equivalent
(c) Hardware Protection – IP 54

Copyright © UTIITSL NCMC Project

13 APPENDIX E: INTEGRATED CONTROL UNIT (ICU)

Integrated Control Unit (ICU) Key features and Specifications

13.1 VTU / ICU Minimum Key Features and Specifications:

(i) GPS/GSM/GPRS/SMS connections

(ii) Remote control via mobile phone or computer

(iii) Fast signal acquisition

(iv) Excellent locating capability under weak signal environment

(v) Locate single waypoint or track continuously

(vi) Locate at preset time interval or real time

(vii) Live tracking on map

(viii) Low power battery alert

(ix) Over speed alarm when vehicle crosses the restricted speed limit

(x) Geo-fence alarm when vehicle exits or enters a predefined area

(xi) Sleep mode when the vehicle is not moving

(xii) Detect working status periodically like heart beat rate when the OBU is in sleep mode

(xiii) Power disconnection alarm when someone cuts off the power line

(xiv) Data stored in flash memory when there is no GPRS and sent when GPRS recovers

(xv) Built-in motion sensor

(xvi) GSM cell ID/ the device ID to which the SIM card is currently attached to optional features:

(a) Two way voice communication

(b) Connect serial port / Ethernet port to devices such as camera, LCD, RFID reader, Validator and printer etc.

Copyright © UTIITSL NCMC Project

13.2 Minimum VTU / ICU Specifications:

GPS Chipset	SIRF Star III or Equi
GSM Module	GSM900/1800/1900 MHz or 850/900/1800/1900 MHz
GPRS Protocol	TCP/UDP
Position Accuracy	10-15 metres
Hot Start	1 second
Warm Start	38 seconds
Cold Start	42 seconds
Antenna GSM/GPS	Internal
Visual Indication	For Power / GSM / GPS
I/O Port	2 switch input ports, 2 analog input ports, 2 digital input ports, 5 digital output ports , 2 serial input ports RS232 and 1 mini USB port
Motion Sensor	Built-in
Flash Memory	16Mb
Microphone/speaker	High sensitivity
Battery	Rechargeable DC 3.7V/1000 mA Li-polymer battery
Power Consumption	Active mode < 100mA,
Exterior Power Supply	DC12V-24V
Operating Temperature	-20°C to + 85 °C
Humidity	Up to 75% non-condensing
Interface	RFID Readers, Temperature, Fuel Sensors,
Certifications	As per attached sheet

Copyright © UTIITSL NCMC Project

13.3 Minimum Certification Required for VTU / ICU

S .No	Standards	Description	Technical Specification (Wherever Applicable)
1	AIS 400	Electromagnetic Radiation from Automotive vehicle-Permissible levels and methods of test	
2	a) EN55022: 2006+A1: 2007 b) EN55024: 1998+A1: 2001+A2: 2003	Certificate of Conformity (CE) with the EC Council Directive of 2004/108/EC. The following aspects are covered under this standard: a) Radiated emission b) Electrostatic Discharge Immunity c) Continuous Radiated Disturbances d) Electrical Fast Transients e) Continuous Conducted disturbances	
3	FCC part 15B	Compliance with part 15B of FCC rules for Radiated emission	
4	SAE J1455/ISO 16750 (For Thermal Shock)	Road Vehicles-Environmental Condition and testing for electrical and electronic equipment	Min temperature: -40 deg C Max temperature: +85 deg C Dwell time: 2 hours No of cycles: 5 Total time: 20 h
5	SAE J1455/ISO 16750 (For Vibration)	Road Vehicles-Environmental Condition and testing for electrical and electronic equipment	5-40Hz, 2G (RMS), 30 hours each axis. Total time 90 hours. However, tested for a total time of 24 hours. Minimum is acceptable.
6	IEC 60529	For Ingress Protection class 65	

Copyright © UTIITSL NCMC Project

14 APPENDIX F: PASSANGER INFORMATION SYSTEM (PIS)

14.1 Passenger Information System (PIS)

This feature consists of:

(a) Bus stop LED display board

(b) Display server application

(c) Server with a broad band USB Data card, Static IP.

14.2 Bus Stop Led Board Specifications

(i) Type of Media: Super Luminosity LED made of AlInGaP material

(ii) No. of sides: 1

(iii) Pitch - minimum 7.5mm

(iv) Line matrix - minimum of 16 rows x 128 columns

(v) No of Lines in the display

(a) 2 Lines in English

(b) Single line in Local language

(vi) LED Type - 4 mm / 5mm Oval – Amber colour

(vii) Wireless interface: GSM, GPRS class 10 (TCP/IP)

(viii) Memory: Minimum capability of 32KB

(ix) Power: 230V AC (nom), 90V (min)

(x) Protocol: TCP/IP, FTP, HTTP

(xi) Color : Amber LEDs

(xii) Wavelength - 590 to 595 nm dominant wavelength

(xiii) Brightness: 600 to 1000 mcd (typ)

(xiv) Viewing Angle – (minimum of) wide viewing angle 120 degree side to side / minimum 60 degree from centre

(xv) Ambient Operating Temp - (-) 10 Deg to (+) 60 Deg. Cel

(xvi) Relative humidity – Up to 95%

(xvii) Visibility – Minimum of 50 feet in all weather conditions. Higher visibility is preferred

(xviii) UV resistance - yes

(xix) Information to be displayed – For Example: Bus route no, Destination (in scrolling text) and Expected time of arrival (hh:mm) and locally stored scrolling messages with watch dog timer

(xx) Local Craft Interface - RS 232 / 485 / USB

(xxi) Display Language – English, Plus any one local Language

Copyright © UTIITSL NCMC Project

(xxii) Display format: To support Fixed messages and scrolling

(xxiii) Display Update - minimum 15 Seconds (Should be configurable)

(xxiv) Automatic brightness control

(xxv) Ingress Protection Grade – Front IP 65, Rear IP54

(xxvi) No of buses to be displayed - as per PIS requirement

(xxvii) Cabinet - MS enclosure, with mounting clamps

(xxviii) Anti Theft mechanisms should be available with SMS

14.3 Display & Display illumination:

All sign displays shall consist of pixels utilizing High Intensity Light Emitting Diodes ("LED"), for superior outdoor environmental performance, of superior UV resistant Epoxy lens and superior resistance to the effects of moisture. Each pixel shall have a dedicated LED for illumination of that pixel in all lighting conditions. The sign system shall have multi-level intensity changes, which adjust automatically as a function of ambient lighting conditions.

This LED shall be mounted such as to be visible directly to the observer positioned in the viewing cone, allowing for full readability for minimum 60 degrees to 120 degrees either side of the destination sign centre line. The LED shall have an operating life MTBF of not less than 100,000 hours.

14.4 Display Monitoring:

A web based display monitoring software has to be provided along with the displays. This shall help to track the displays performance on a daily basis. The software shall provide reports for the ETA displayed at a Bus stop and shall also provide reports on data that did not reach the remote display. The software shall indicate if any remote display is not communicating with the display server. Using the software Synchronization of Time shall be achieved for all displays that are installed.

14.5 Communication with PIS Board:

PIS should communicate via the Internet to Vehicle Tracking System (VTS) Client Workstations and VTS Servers. At the sign level, information should be processed through the controller board to the onboard modem (GPRS/GSM, EVDO/CDMA/1XRT) fitted with the display unit.

14.6 Internal antenna:

The Outdoor PAS should have an internal antenna that cannot be damaged during shipping and cannot be tampered with as it is inside the assembly of the sign. The dual band (900/1900 MHz) antenna strip should be of Unity gain, 50 ohm, 5 Watt covert antenna that is protected by tamper proof endplates. It should plug directly into the internal modem (GPRS/GSM, EVDO/CDMA/1XRT).

Copyright © UTIITSL NCMC Project

14.7 Power supply:

The outdoor display unit shall be powered by Alternating Current (AC) or Direct Current (DC) with an option to Solar Power. AC options are 120 volt (50/60 Hz-3 Amp. max) or 240 volt (50/60 Hz, 2 Amp max).

If a solar powered option is used the sign will utilize 12 or 24 volt input. The solar panel is also optional. Power input to the signage should be done with a single opening, liquid tight connection on the rear of the sign.

14.8 Electronic System Requirements:

The display system components shall be certified to have been subjected to a "burn-in" test of a minimum of twelve (12) hours operation in a temperature of 60 degrees C prior to final inspection.

Copyright © UTIITSL NCMC Project