RKF Travel Card
Requirement Specification

CONTENTS

1 INTRODUCTION

1.1 Scope

This document specifies the functional and contents requirements of the RKF travel card. The requirements comprise a range of useful application objects, e.g. purse, ticket and contract.

The intention of this requirement specification is to be card technology independent. The technical requirements for selected IC-card technologies are specified in [RKF-0021].

Separate documents specify how this requirement specification is implemented using the card technologies specified in [RKF-0021].

1.2 Reader's Guide

Chapter 2 gives an overview of the RKF travel card.

Chapter 3 to 5 define requirements for the 3 layers of the RKF travel card:

- Card issuer layer
- Travel card support layer
- Travel card applications layer

Chapter 6 defines security requirements.

The requirements that are defined in this document are divided in two categories. *Shall* requirements are mandatory requirements. These requirements are necessary for the travel card to be compatible between implementations. *Should* requirements are not mandatory but are still very relevant because they support the interoperability of the travel card between PTAs.

The requirements of chapters 3 to 5 do not directly include requirements of specific data elements within system objects or application objects. Instead, required data elements and data element groups are specified in [RKF-0023] (section 'Data Element Groups'). Required data elements are marked G or G/T1:

G: General data type, same representation for all card technology types.

G/T1: General data type, representation depends on card technology, representation for type 1 is shown in [RKF-0023].

2 OVERVIEW OF THE RKF TRAVEL CARD

This chapter gives an overview of the travel card based on the layers, that are used throughout the travel card specification.

2.1 General Overview

The purpose of the RKF travel card is to facilitate one travel card within the public transport in the Nordic countries. The co-operation concerns the card technologies (e.g. technologies with or without contacts) and the RKF travel card application objects (e.g. purse, ticket and contract).

The objectives are that the RKF travel card shall offer a useful platform for PTAs implementing IC-card travel cards in either of 2 situations:

- The travel card is used locally by one PTA
- The travel card is used by a group of co-operating PTAs

The travel card is defined by a number of layers. A layer has its own defined functionality and defined interfaces to superior and subordinate layers.

Figure 1 (see below) shows the layers and their relations. This requirement specification defines relevant requirements on the layers:

- Technical layers (defined in [RKF-0021])
- Card issuer layer
- Travel card support layer
- Travel card applications layer

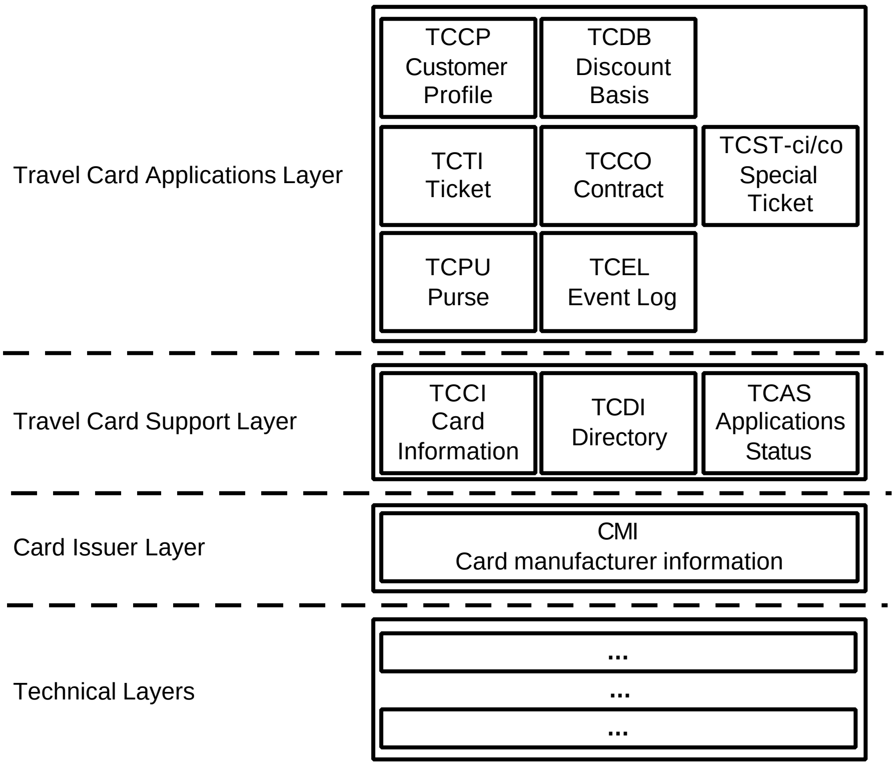

Figure 1: RKF travel card systems overview

2.2 Overview of Technical Layers

Technical layers of the type 1 RKF travel card are defined in [RKF-0021].

2.3 Overview of the Card Issuer Layer

The card issuer layer offers a general platform where several and different card applications can co-exists, for example an electronic purse, issued by a bank, and a public transport application.

The layer manages the overall allocation of resources on the card platform. The layer:

- Includes a directory function that manages valid card applications.
- Includes information about the responsible card Issuer.
- Includes information about the unique card serial number of the physical card.
- Functions according to rules and guidelines that are defined by the card issuer, concerning for example security and resource allocation.

2.4 Overview of the Travel Card Support Layer

The main purpose of the travel card support layer is to support and manage the travel card application objects, including for example purse, tickets and contracts. The layer:

- Includes a directory function, and an applications status function, that supports and manages the travel card applications.
- Functions according to rules and guidelines that are defined by the travel card support layer.

2.5 Overview of the Travel Card Applications Layer

This specification specifies 7 types of RKF travel card application objects:

- Travel card purse (TCPU)
- Travel card event log (TCEL)
- Travel card contract (TCCO)
- Travel card ticket (TCTI)
- Travel card special tickets (TCST)
- Travel card customer profile (TCCP)
- Travel card discount basis (TCDB)
- Travel card reservation (TCRE)

All travel card application objects or other applications within the travel card support layer shall:

- Have a responsible provider
- Include a unique identifier
- Utilise the common resources within the travel card support layer according to defined rules.

2.6 The RKF Travel Card in an Automatic Fare Collection System

The travel card shall offer a flexible and secure card platform that can operate in different public transport systems for automatic fare collection.

The model outlined in figure 2 describes the system environment that the travel card shall operate in.

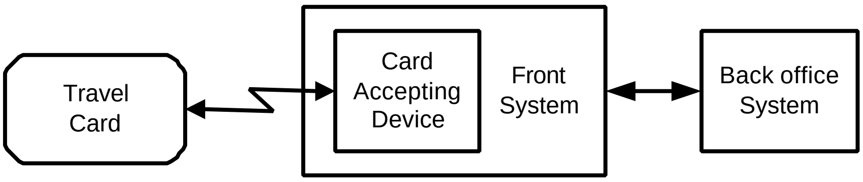

Figure 2: Travel card system environment

In a specific automatic fare collection system, a number of requirements have to be further identified and defined, for example:

- Customer services for example possibilities to view the contents of the public transport application including the contents of the event log.
- Procedures for validating tickets and contracts. For example the customer should first present the card to the reader and then give relevant information via the implemented user interface, for example tell the driver the destination or press relevant buttons.
- A signal that indicates that for example a load transaction is completed.
- Signals and lights could indicate that something went wrong and that the transaction was cancelled.
- A green light could indicate that everything is Ok.
- The time-outs for not completed transactions. If no activity is performed, the transaction should be cancelled.
- Relevant customer error messages should be shown.
- Transaction speed requirements
- The connection between front systems and the back office system must be specified. This connection might not be on-line. For example in moving vehicles, the front systems might only perform exchange information with the back office system once a day.

This type of requirements are very important to define. They are, however, outside the scope of this specification and [RKF-0021], and are therefore not further defined here.

3 CARD ISSUER LAYER

This chapter describes the requirements of the card issuer layer

3.1 The Card Issuer Layer

3.1.1 Definition

The card issuer layer is the layer that represents the card, i.e. facilitates that several and different card applications can co-exist on one card. The layer defines the allowed applications on the card and rules and guidelines for the usage of the card resources.

3.1.2 Requirements

The card issuer layer could represent any card. The travel card requires general smart card functionality from the card issuer layer.

Identification and Administrative Data

- The card shall include a unique serial number.
- The card shall include information about the responsible issuer of the card. The identification information shall be unique within a defined context.

Security and Accountability

- Only authorised users shall be allowed to access the contents and resources of the card.
- Authorised users should be allowed to add or delete card applications in the card issuer layer.
- It shall be possible to define different access rights to information and resources on the card. This should be possible to specify both for different function types and different user types.
- It shall be possible to detect when information on the card is corrupt. It should be possible to correct this information.
- Authorised users shall be able to block the card. When a card is blocked no resources are accessible on the card.
- Authorised users shall be able to unblock a blocked card.

Usage and Validity

- The resources and the contents of the card/card issuer layer shall be managed by a shared directory function.
- The directory function shall include information about the stored card applications and their location on the card.

3.1.3 Contents

The card issuer layer shall include:

- A directory function
- A unique card serial number
- Information about the card Issuer
- The card expiration date

4 TRAVEL CARD SUPPORT LAYER

This chapter describes the requirements of the travel card support layer

4.1 The Travel Card Support Layer

4.1.1 Definition

The RKF travel card support layer is a defined set of RKF travel card system objects that manage the RKF travel card application objects:

- The card information holds static information common to all system and application objects.
- The directory of the layer describes the actual system and application objects of the travel card. This directory is separated from the superior directory function in the card issuer layer.
- The applications status function controls the update of application objects to ensure indivisible transactions.

4.1.2 Requirements

The travel card support layer manages travel card application objects. The application objects can be of different types, e.g. purse, tickets or contracts. Requirements on the travel card support layer are:

Identification and Administrative Data

- The travel card support layer can be one of several layers/branch applications on one card. The travel card application shall have one unique application identifier.

Security and Accountability

- Authorised users should have the possibility to add and remove travel card application objects on the travel card support layer.
- The read and update access to application objects and specific data element groups should be possible to regulate.
- It should be possible to define access rights (read and update) based on the user type and/or the transaction type.
- Authorised users shall be able to block the travel card support layer.
- Authorised users shall be able to unblock a blocked travel card support layer.

Usage and Validity

- The layer can include several valid contracts and tickets at any given time. It should be possible to find information about the validation order of these application objects within the travel card support layer.
- Authorised users should have the possibility to change the validation order of the application objects within the travel card support layer.

4.1.3 Contents

- The travel card support layer shall include unique identification of the travel card support layer
- The travel card support layer should include the validation order within the travel card support layer

4.2 TCCI: Travel Card Card Information

4.2.1 Definition

The card information (TCCI) is a system object of the travel card support layer. The TCCI holds static information common to all system and application objects, i.e. information that is not changed in normal validation transactions.

4.2.2 Requirements

Identification and Administrative Data

- The TCCI shall include information about the responsible provider. The identification information shall be unique within the context of the travel card support layer.
- The TCCI shall include information about the current version of the travel card support layer.

Security and Accountability

- No specific requirements.

Usage and Validity

- The TCCI shall manage static information common to the support layer and the applications layer of the travel card.

4.2.3 Contents

- The TCCI shall include information about the travel card support layer provider
- The TCCI shall include information about which version of the travel card support layer that is written to the card.
- The TCCI shall include information about the status of the travel card support layer.
- The TCCI shall include the data elements marked ‘G’ or ‘G/T1’ of the TCCI data element group described in [RKF-0023].

4.3 TCDI: Travel Card Directory

4.3.1 Definition

The directory function (TCDI) is a system object of the travel card support layer. The TCDI describes the actual system objects and application objects of the travel card to facilitate correct and effective access to these objects.

4.3.2 Requirements

Identification and Administrative Data

- The TCDI shall include relevant information about every system and application object within the layer. The information shall include:
  - the application provider, i.e. the user that is responsible for the application object
  - the type of application, e.g. the purse
  - information about the location of the application object on the card

Security and Accountability

- No specific requirements.

Usage and Validity

- The contents and resources of travel card support layer and the travel card applications layer shall be managed by the TCDI.

4.3.3 Contents

- The travel card support layer shall include a TCDI.
- The TCDI shall include the data elements marked ‘G’ or ‘G/T1’ of the TCDI data element group described in [RKF-0023].

4.4 TCAS: Travel Card Applications Status

4.4.1 Definition

The applications status function (TCAS) is a system object of the travel card support layer. The TCAS controls the update of application objects to ensure indivisible transactions. I.e. the TCAS shall enable a well-defined commitment of transactions involving one or more application objects: all card updates of a transaction are either completed totally or not carried out at all.

4.4.2 Requirements

Identification and Administrative Data

- The TCAS shall include relevant information about every application object to ensure indivisible transactions.

Security and Accountability

- No specific requirements.

Usage and Validity

- The TCAS shall provide facilities for ensuring indivisible transactions.

4.4.3 Contents

- The TCAS shall include the data elements marked ‘G’ or ‘G/T1’ of the TCAS data element group described in [RKF-0023].
- The contents of TCAS is expected to be dependent on the choice of card technology.

5 TRAVEL CARD APPLICATIONS LAYER

This chapter describes the requirements of the travel card applications layer

5.1 TCPU: Travel Card Purse

5.1.1 Definition

The travel card purse (TCPU) application object holds the balance of the customer's account. The TCPU is used for payments of travel card tickets, contracts, or other items.

The TCPU includes a balance value. This value is expressed in a unit and a currency. The value of the TCPU decreases when the customer buys a ticket with the TCPU. The value of the TCPU increases when a customer charges the TCPU with more units.

The TCPU can never be used as a ticket or a contract.

If the TCPU is present, it may be shared by all PTAs using the travel card.

5.1.2 Requirements on Travel Card Purse

The following requirements concern the TCPU:

Identification and Administrative Data

- The TCPU shall include information about the responsible provider.
- The TCPU shall have a unique identifier within the context of the travel card support layer.
- The TCPU shall include information about which version of the TCPU it represents.
- The TCPU shall include an actual value. It shall be possible to express this value in a defined currency and a unit.
- The TCPU should include a deposit value. It shall be possible to express this value in a defined currency and a unit.
- The TCPU shall have a defined period of validity. The validity period shall be defined by two dates, i. e. the initialisation date and the last recharge date.
- The TCPU shall include the data elements marked 'G' or 'G/T1' of the TCPU data element groups described in [RKF-0023].

Security and Accountability

- The TCPU shall include functionality that makes it possible to achieve accountability concerning the usage of the TCPU.
- The TCPU shall include functions that can guarantee that only authorised users have manipulated with the contents of the TCPU.
- The read and update access to data element groups within the TCPU shall be regulated. It should be possible to define access rights (read and update) per user or card transaction.
- It shall be possible for authorised users to block the TCPU.
- It shall be possible for authorised users to unblock the TCPU.

Usage and Validity

- The travel card shall contain one TCPU or no TCPU.
- It shall be possible to use the TCPU as a pay method when buying travel card ticket and travel card contracts or other items.
- The TCPU shall be impersonal.
- It should be possible for the PTA to add extra PTA specific functionality to the TCPU without compromising the travel card functionality of the TCPU.

5.2 TCEL: Travel Card Event Log

5.2.1 Definition

The event log (TCEL) application object is an optional function that records defined transactions to applications involving one or more application objects. The recorded information can be used for tracking, inspecting and verifying the quality of the support and application layers.

If the event log is present, it is shared by all users of the travel card.

The event log contains a number of log records.

A log record is a defined set of information written to the card when certain events are happening to the card.

5.2.2 Requirements

If a travel card contains a TCEL, it shall be initiated when the travel card support layer is initiated.

Identification and Administrative Data

- The shared event log function shall have a unique identifier.
- The TCEL shall include information about the responsible provider. The identification information shall be unique within the context of the travel card support layer.
- It shall be possible to uniquely identify each log record within the context of the travel card support layer.

Security and Accountability

- Authorised users shall be able to add and remove log records in the event log function.
- The read and update access to the log records and specific data elements within a log record should be possible to regulate.
- It should be possible to define access rights (read and update) based on the user type and/or the transaction type.
- It shall be impossible to modify an already written log record.

Usage and Validity

- The TCEL shall include information that informs the users where to update/read relevant log records.
- The TCEL shall include the following information about the written log records:
  - the issuer of the log record, i.e. the user that wrote the log record
  - the type of log record, e.g. payment with the purse
- The log records shall be used in a first-in-first-out (FIFO) order.
- If present, the TCEL should store at least ten log records.

5.2.3 Contents

- Information about the responsible TCEL provider.
- Unique identifier for the TCEL.
- Version number for the TCEL.
- Information about where to read or update next log record.
- Every log record shall a least include the following information:
  - date and time
  - issuer
  - sale device
  - information about the event
  - serial number
  - result of the transaction

- The TCEL log records shall include the data elements marked 'G' or 'G/T1' of the *Event Log Record* data element group described in [RKF-0023].

5.3 TCTI: Travel Card Ticket

5.3.1 Definition

A travel card ticket (TCTI) application object can hold a valid ticket for a specific journey. The validity of the TCTI is defined in the TCTI with its attributes and the defined rules to interpret these attributes.

The TCTI is validated when the journey is carried out. The TCTI can be validated several times during one journey. The TCTI can be updated/modified during a journey. The validity of the TCTI can be changed.

A TCTI can be issued in two ways, it can be bought with a TCPU or any other pay method (e.g. cash) or it can be issued when validating a contract.

5.3.2 Requirements on the TCTI

The following requirements concern the TCTI:

Identification and Administrative Data

- The TCTI shall have a unique identifier within the context of the travel card support layer.
- The TCTI shall have a responsible TCTI provider.
- The issuer of the TCTI is not necessarily the same as the TCTI provider. Information about the issuer shall be included in the TCTI.
- The TCTI shall include the data elements marked 'G' or 'G/T1' of the TCTI data element groups described in [RKF-0023].

Security and Accountability

- The TCTI shall include functions that can guarantee that only authorised users have manipulated with the contents of the TCTI.
- The read and update access to attributes within the TCTI shall be regulated. It should be possible to define access rights (read and update) per user or card transaction.
- It shall be possible for authorised users to block a TCTI.
- It shall be possible for authorised users to unblock a TCTI.

Usage and Validity

- The TCTI should contain information about the pay method or the contract that was used for the purchase of the TCTI.
- The TCTI should include information about its validity.
- It shall be possible to validate, including update, the TCTI on check-in to and/or on check-out from for example a vehicle or a terminal.
- The TCTI should include the possibility to have the following validity constraints:
  - It should be possible to include one or several free interchanges between the start point and the end point of a journey.
  - It should be possible to define a valid passenger group that are allowed to make use of the TCTI. The passenger group consists of one or more passenger types and one or more passengers of each passenger type.
  - It should be possible to define the validity concerning e.g. route numbers, zones and distance.
  - It should be possible to define different vehicle classes that are allowed with the TCTI.
  - It should be possible to define the validity during a time period, i.e. the TCTI should be valid from date and time to date time or valid for a certain run.
- The TCTI should have a price. This price is expressed in a currency and a unit.
- It should be possible to issue the TCTI in advance or when the journey is taking place.

5.4 TCCO: Travel Card Contract

5.4.1 Definition

A travel card contract (TCCO) application object can include privileges to issue tickets with certain validity. Tickets that are issued with a TCCO have validity constraints based on the validity constraints defined in the TCCO.

A TCCO is not a ticket. It can, however, represent a period card allowing the customer to carry out journeys without issuing a ticket.

5.4.2 Requirements

The following requirements concern the TCCO:

Identification and Administrative Data

- The TCCO shall have a unique identifier within the context of the travel card support layer.
- The TCCO shall have a responsible TCCO provider.
- The TCCO shall include the data elements marked ‘G’ or ‘G/T1’ of the TCCO data element groups described in [RKF-0023].

Security and Accountability

- The TCCO shall include functions that can guarantee that only authorised users have manipulated with the contents of the TCCO.
- The access to attributes within the TCCO shall be regulated. It should be possible to define access rights (read and update) per user or card transaction.
- It shall be possible for authorised users to block the TCCO.
- It shall be possible for authorised users to unblock the TCCO.

Usage and Validity

- The TCCO should include information about its validity.
- It should be possible to validate, including update, the TCCO on check-in to and/or on check-out from for example a vehicle or a terminal.
- The TCCO should include the possibility to have the following validity constraints:
  - It should be possible to include one or several free interchanges between the start point and the end point of a journey.
  - It should be possible to define a valid passenger group that are allowed to make use of the TCCO. The passenger group consists of one or more passenger types and one or more passengers of each passenger type.
  - It should be possible to define the validity concerning for example route numbers, zones and distance.
  - It should be possible to define different vehicle classes that are allowed with the ticket.
  - It should be possible to define the validity period (in time), i.e. the TCCO shall be valid from date and time to date and time or valid for a certain run.
  - It should be possible to define validity periods within the validity period, e.g. restrictions concerning certain days in the week, certain hours in a day or number of journeys during one day.
  - It should be possible to not predefine the validity start date of a TCCO, i.e. the validity starts when the customer uses the TCCO for the first time.
  - It should be possible to record loyalty points, in a TCCO, on which the price of a journey will be based.

- The TCCO should have a price. This price is expressed in a currency and a unit.
- It should be possible to issue the TCCO in advance or when the journey is taking place.

5.5 TCST-ci/co: Travel Card Special Ticket (ci/co)

5.5.1 Definition

A travel card special ticket (ci/co) application object is an example of the implementation of the travel card special ticket (TCST) concept described in section 'TCST Concept' of [RKF-0022]. The TCST concept allows PTAs, under certain conditions, to design a ticket application object that meets their needs better than TCTI.

The TCST-ci/co represents a ticket specially suited for check-in/check-out validation. The validation status of the ticket is open after check-in at the origin of the journey, and closed after check-out at the destination of the journey.

A TCST-ci/co is not issued in connection with any contract or ticket application (e.g. TCCO and TCTI).

A TCST-ci/co application object can be created in different ways by the issuing PTA but it shall adhere to the specification of the TCST concept.

5.5.2 Requirements

The following requirements concern the TCST-ci/co:

Identification and Administrative Data

- The TCST-ci/co shall have a unique identifier within the context of the travel card support layer.
- The TCST-ci/co shall have a responsible TCST-ci/co provider.
- The issuer of the TCST-ci/co is not necessarily the same as the TCST-ci/co provider. Information about the issuer shall be included in the TCST-ci/co.
- The TCST-ci/co shall include the data elements marked 'G' or 'G/T1' of the TCST-ci/co data element group described in [RKF-0023].

Security and Accountability

- The TCST-ci/co shall include functions that can guarantee that only authorised users have manipulated with the contents of the TCST-ci/co.
- The read and update access to attributes within the TCST-ci/co shall be regulated. It should be possible to define access rights (read and update) per user or card transaction.
- It shall be possible for authorised users to block a TCST-ci/co.

- It shall be possible for authorised users to unblock a TCST-ci/co.

Usage and Validity

- The TCST-ci/co shall include information about its validity.
- It shall be possible to validate, including update, the TCST-ci/co on check-in to and/or on check-out from for example a vehicle or a terminal.
- The TCST-ci/co shall include the possibility to have the following validity constraints:
  - It shall be possible to define a valid passenger group that are allowed to make use of the TCST-ci/co. The passenger group consists of one or more passenger types and one or more passengers of each passenger type.
  - It shall be possible to record the actual validation status.
  - It shall be possible to record the place and time of check-in and check-out validations.
  - It should be possible to record place and time of control validations.
  - It should be possible to possible to record information to enable excess fare calculation.
- The TCST-ci/co shall have a price. This price is expressed in a currency and a unit.
- It shall be possible to issue the TCST-ci/co when the journey is taking place.

5.6 TCCP: Travel Card Customer Profile

5.6.1 Definition

A travel card customer profile (TCCP) application object shall contain information identifying the passenger or group of passengers travelling with the card. It is not a mandatory part of the travel card, but should be an option for PTAs to base their application objects upon. It shall be possible to describe three different passenger types and a number of passengers of each type.

The TCCP shall as well contain information regarding the preferences of the customer such as the preferred language, preferred type of dialogue.

The TCCP shall be able to describe a customer's subscription or credit agreement with a PTA.

The TCCP is used whenever an application object on the card needs to take the customer profile into account.

5.6.2 Requirements

The following requirements concern the TCCP:

Identification and Administrative Data

- The TCCP shall have a unique identifier within the context of the travel card support layer.
- The TCCP shall have a responsible TCCP provider.
- The issuer of the TCCP is not necessarily the same as the TCCP provider. Information about the issuer shall be included in the TCCP.
- The TCCP shall include the data elements marked ‘G’ or ‘G/T1’ of the TCCP application object described in [RKF-0023].

Security and Accountability

- The TCCP shall include functions that can guarantee that only authorised users have manipulated with the contents of the TCCP.
- The read access to attributes within the TCCP shall be regulated. It should be possible to define access rights (read) per user or card transaction.
- It shall not be possible to update the information in a TCCP except when initiating the TCCP application object.
- It shall be possible for authorised users to block a TCCP.
- It shall be possible for authorised users to unblock a TCCP.

Usage and Validity

- The TCCP shall include information about its validity/status.
- The travel card can contain one TCCP or no TCCP.

5.7 TCDB: Travel Card Discount Basis

5.7.1 Definition

The TCDB (travel card discount basis) application object accumulate information about the use of the travel card and thereby provide the basis for fare calculation taking an acquired level of discount into account. It shall be able to contain information about the use of the card for a period of at least three periods (e.g. months), and it shall store at least two counters for the current period - one low precision counter and one high precision counter.

5.7.2 Requirements

The following requirements concern the TCDB:

Identification and Administrative Data

- The TCDB shall have a unique identifier within the context of the travel card support layer.

- The TCDB shall include information about which version of the TCDB it represents
- The TCDB shall contain information about the use of the card for a period of at least three periods.
- The TCDB shall store at least two counters for the current period - one low precision counter and one high precision counter
- .The TCDB shall have a unique identification of the period for which the counters accumulate information, so that it can be identified when a change of period has happened since the last use of the card.
- The TCDB shall include the data elements marked ‘G’ or ‘G/T1’ of the TCDB data element groups described in [RKF-0023].

Security and Accountability

- The TCDB shall include functions that can guarantee that only authorised users have manipulated with the contents of the TCDB.
- The read and update access to data elements groups within the TCDB shall be regulated. It should be possible to define access rights (read and update) per user or card transaction.
- It shall be possible for authorised users to block the TCDB.
- It shall be possible for authorised users to unblock the TCDB.

Usage and Validity

- The TCDB shall include information about its validity/status.
- The travel card can contain one TCDB or no TCDB.
- The TCDB shall be impersonal and deal with the activity of use of the card rather than the activity of a specific person.
- The travel card shall contain one TCDB or no TCDB.

5.8 TCRE: Travel Card Reservation

The reservation application object is not specified yet. The application object is reserved for later use.

6 SECURITY REQUIREMENTS

6.1 General

The RKF travel card application is a set of data and related functions that can be stored in a card. The travel card support layer shall be self-contained, meaning that it shall be possible to move the data and the functions from one card environment to another. Different operating environments shall not change the functionality of the travel card support layer. The travel card support layer will therefore only use standard smart card functions, including security functions.

The layer shall be able to either exist by itself or coexist with other/different application objects in one card without any integrity loss.

The relevant security requirements are defined in the following areas

- Smart card security requirements
- Information security requirements

Relevant security requirements are also defined per information and function within the travel card support layer.

6.2 Smart card security requirements

6.2.1 Personalisation

Electronic personalisation is the process whereby an application is defined according to [ISO 7816-4]. General data related to the card and the travel card support layer is written to the card e.g. file tree format, necessary files (MF, DFs and EFs) and file structures. Security restrictions are also defined for the generated files. All provider and application specific information is also written to the card, for example secret card specific keys.

The personalisation of the card shall be performed in a secure way.

The personalisation of the travel card shall only be performed once.

6.2.2 Secure Messaging

Secure Messaging aims to ensure authenticity, and if necessary the confidentiality of all or some of transmitted data between the card and the CAD.

Secure Messaging shall be applied to the transmission of data between the card and the CAD according to [ISO 7816-4].

6.2.3 Authentication

The authentication of the user shall be based on authentication according to [ISO/IEC 9798-2].

The authentication of the card shall be based on authentication according to [ISO/IEC 9798-2].

6.2.4 Card Blocking

- It shall be possible to block the card.
- It shall be possible to unblock the card.

6.3 Information Security Requirements

The information that is stored within the travel card support layer shall be protected from unauthorised or unintentional modifications.

The protection shall be applicable on the file level.

6.3.1 User Authentication and Data Integrity

Securing the information that is stored within the travel card applications objects concerns data integrity and authentication of the users and data origin. Data integrity and user authentication is achieved by using a MAC (Message Authentication Code). The MAC is computed by applying a hash mechanism to the information that shall be protected and then sign/encrypt the result with a secret key. This key is derived from a master key.

Information owners within the travel card support layer shall define which information that shall be protected with a MAC.

MAC shall be implemented according to [ISO/IEC 9797].

6.3.2 Protection Against Corrupt Information

It shall be possible to detect, if the card has become inconsistent. The card should have functions for detection and correction of unintentional modifications of data on the card.

6.3.3 Key and Security Management

6.3.3.1 Master keys

Each master key shall have a unique identifier and a version indication.

6.3.3.2 Secret Keys for MAC and Authentication

Each card shall have its own unique Secret key for MAC calculation.

Each card shall store information about the algorithm that has been used and a master key identifier belonging to the key that has been used in the MAC calculation.

Each card should have its own unique Secret key for authentication.

6.3.3.3 Key Exchange

It shall be possible to continuously change the key (master key). This means that the keys shall include a version number and it shall be possible to store several generations of keys within the card.

6.3.4 Approved Cryptographic Algorithms

6.3.4.1 Symmetric Algorithms

DES shall be the default symmetric key algorithm used in the Public transport layer to protect sensitive information from unauthorised users. DES is standardized in [ISO 8731-1], [ISO 8372], and [ISO/IEC 10116]. DES can be used both for encryption/signing of information and for the calculation of MAC.

DES shall be used either in the DES-CBC mode, FIPS 81 - National Institute of Standards and Technology (NIST) or the Triple DES mode FIPS 81 - National Institute of Standards and Technology (NIST).

6.3.4.2 Hash Algorithm

Requirements for the hash function are that the number of possible output of the function is sufficiently large and uniformly distributed to prevent an exhaustive key search on the secret key. desMAC shall be used as the default hash algorithm, FIPS 113 - National Institute of Standards and Technology (NIST).

6.4 Travel card information security requirements

The information handled and stored within the travel card support layer shall be available for authorised users.

Each set of data in the card shall have an information owner. The information owner is responsible for the usage of the information. The owner shall also define access rights for other users. This is performed in the personalisation phase.

Information type	Information owner
Card issuer layer • Directory information • Card issuer identifier • Card expiration date • Card serial number	Card issuer
Travel card support layer • TCCI • TCDI • TCAS	Travel card support layer provider
Travel card applications layer Examples: • TCPU • TCEL • TCTI • TCCO • TCST • TCCP • TCDB • TCRE	Travel card application providers

6.4.1 Card Issuer Layer

The information stored in the card issuer layer is static. It is written once, in the personalisation phase, and after that it shall not be modified.

6.4.2 Travel Card Support Layer

The information that is handled and stored in the travel card support layer is both dynamic and static. The information that is static is for example information about the support layer provider, the version indication, the unique identifier etc. This information shall not be changed after it has been written to the card. All authorised users to the travel card support layer shall have read access to this information.

Common information that is dynamic within the travel card support layer information is the directory function, the validation order information, and the log records of the event log. The log record information is also dynamic. The information owner is responsible for the usage of and the definition of access rights to this information.

Information	Read	Update
TCCI	Authorised users with access rights to the travel card support layer	Users with the access rights to modify/update/delete applications within the travel card support layer
TCDI	Authorised users with access rights to the travel card support layer	Users with the access rights to modify/update or delete applications within the travel card layer
TCAS	Authorised users with access rights to the travel card support layer	Users with the access rights to update application objects within the travel card applications layer
TCEL	Authorised users with access rights to the travel card support layer	Users with the access rights to modify/update/delete application objects within the travel card support layer
Travel card application objects	Authorised users with access rights read an identified travel card application	Users with the access rights to modify/update/delete application objects within the travel card support layer. All application objects shall be protected with MAC. MAC shall be applied to the information content of the applications.