Prepared by	Document id	Version	Document date
	RKF-0017	1.00	29 May 2001

RKF Travel Card – Volume B
Introduction

CONTENTS

1 INTRODUCTION

The RKF Travel Card is issued by an association called “Resekortsföreningen i Norden”. The members of the association are public transport authorities in Denmark, Norway and Sweden.

The purposes of the association are to establish and maintain standards that ensures interoperability between public transport associations regarding fare regulations, smart card based tickets, settlement procedures of income, etc.

This specification set up handles the standard of tickets based on a smart card platform.

1.1 Purpose

The purposes of this specification set up are:

- To establish a common specification for implementation of smart cards within public transport authorities of the Nordic countries.
- Enable a certain degree of interoperability, in terms of tickets, between the public transport authorities.
- To communicate the requirements of smart card based tickets to suppliers.
- To form a base for future changes of requirements.

2 PURPOSE OF THIS DOCUMENT

The purposes of this document are:

- An introduction to the specifications of the RKF Travel Card.
- Description of revision history of the specifications.
- Explain the internal relations of the specifications.
- A glossary of terms an abbreviations that are used within the specifications.
- How references are made to other documents and standards.

3 REVISION HISTORY

This version of the documentation set up that comprises the specifications handling the RKF Travel Card issued by Resekortsföreningen i Norden is of volume B.

Volume B comprises the following documents:

Document	Document id	Version
RKF Travel Card – Volume B Introduction (this document)	RKF-0017	1.0
RKF Travel Card Requirement specification	RKF-0020	1.0
RKF Travel Card Technical Requirement Specification	RKF-0021	1.0
RKF Travel Card Implementation Specification Type 1	RKF-0022	1.0
RKF Travel Card Implementation Specification Details Type 1	RKF-0023	1.0
RKF Travel Card Implementation Specification Details Type 1 (This document is a excel-formatted version of ref [RKF-0023])	RKF-0025	1.0
RKF Travel Card Implementation Guide Type 1	RKF-0024	1.0
Setting of keys and application identifiers - Edition A[1]	RKF-0018	1.0
Setting of keys and application identifiers - Edition B[1]	RKF-0019	1.0

1 The difference between the documents “Setting of keys and application identifiers edition A and B” is that edition A holds information that should be kept secured. In edition B this information is erased.

Edition A is only for use and distribution to members of Resekortsföreningen and suppliers of ticketing systems that have an established relation to any member of Resekortsföreningen. Edition B is for public use and distribution.

Previous volumes of the RKF Travel Card are:

Volume	Document	Version
A	“Co-operate” public transport card Requirement specification - Application	1.1
	“Co-operate” public transport card Requirement specification Application Appendix A - Concepts and definitions	1.1
	“Co-operate” public transport card Technical Requirement specification	1.1
	“Co-operate” public transport card Implementation specification “Co-operate” public transport card type 1	1.1
	“Co-operate” public transport card Implementation specification “Co-operate” public transport card type 1 Appendix A - Data types	1.11
	“Co-operate” public transport card Implementation guide for standard card according to the “co-operate” public transport card - Type 1	1.11

Volume A has been common known as the “SLTF-specification”.

3.1 Hierarchy of documents

The hierarchy of the documentation set up according to this volume (Volume B) is:

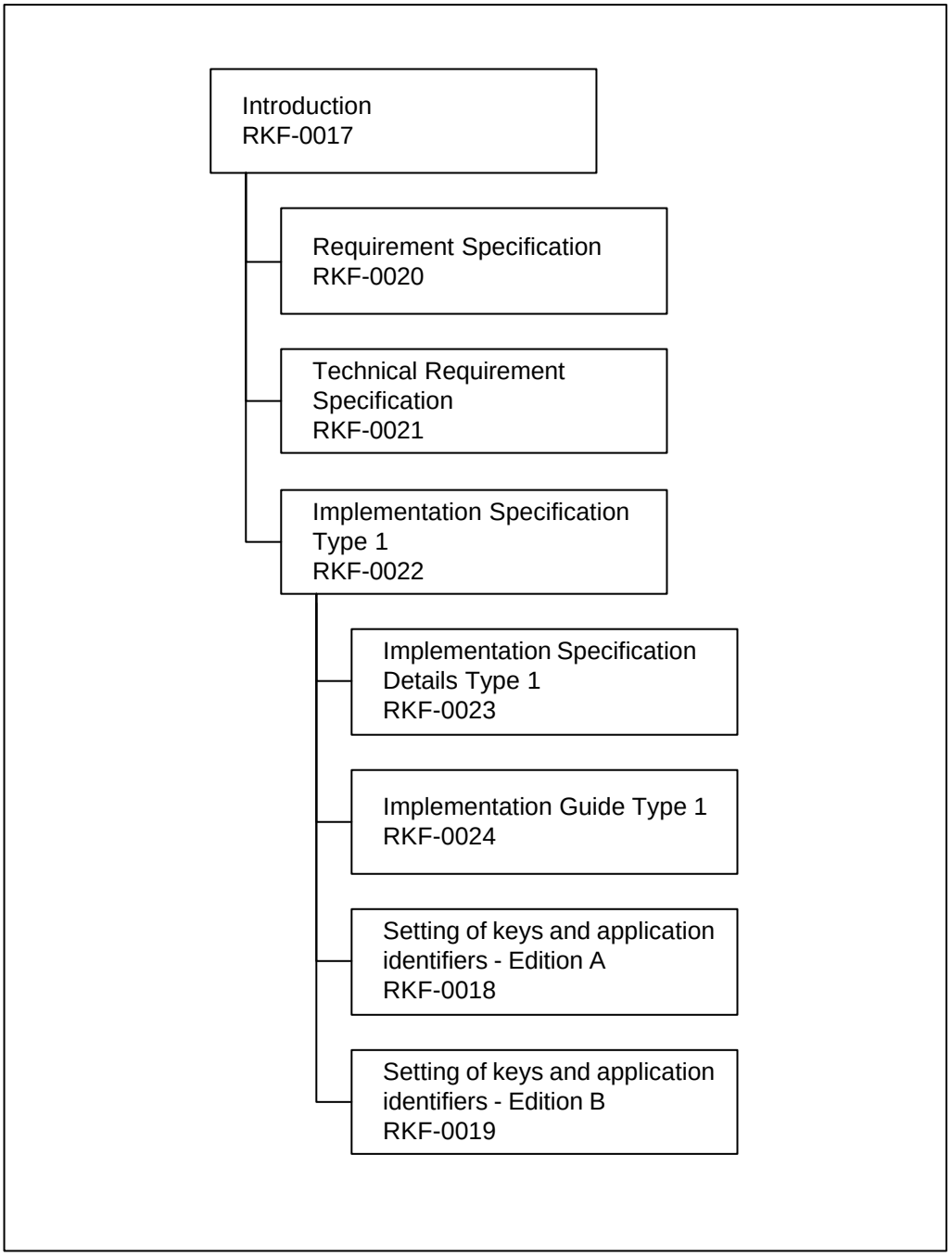

Figure 1 Hierarchy of the documentation set up

4 GLOSSARY

The following terms and abbreviations are used in the documentation set up:

Term or abbreviation	Explanation
AFC	Automatic Fare Collection
AID Application Identifier	A registered identifier unique to the RKF travel card. All PTAs (and some groups of PTAs) have their own AID to identify their applications.
Amount	The price of for example a CPTT or a CPTC is defined by the amount. The amount is the sum (in a currency and a unit) that the customer has paid when buying public transport applications or loading his CPTP.
Application element	See section 4.1.
Application object	See section 4.1.
Authorised user	An authorised user is a user with the authority to perform defined transactions to the travel card applications, according to assigned access rights.
b	Bit
B	Byte
Back office system	The back office system is the part of the ticket system that is normally placed inside the office of the PTA. The back office system takes care of data (e.g. revenues) coming from the front system and gives data (e.g. configuration, black-listing, AFC data and software) to the front system.
Block	1 block contains 16 bytes. This only applies for RKF type 1 cards.
Blocking	Transaction that temporarily disables an application on the card or the card itself from further update of the blocked area. See “Unblocking”.
CAD Card Accepting Device	The card accepting device is the part of the front system that communicates directly with the card.
Cancelling	Card transaction that returns a completed transaction i.e. after cancelling a transaction the card contents should be the same as before the transaction was executed, except for an extra TCEL log record. Example: If a customer gives the wrong destination at purchase, the purchase of a ticket must be cancelled and a new purchase will be executed.
Card application	A multifunction IC-card can hold one or more card applications. The RKF travel card can be one of these card applications
Card issuer	The organisation that issues travel cards to customers and initialises them.

Term or abbreviation	Explanation
Card issuer layer	Co-ordinates different card applications on one card. This is the superior layer of the card.
Charging	Card transaction that increases the value of the TCPU with an amount.
Co-operate public transport card	See “RKF travel card”.
Co-operate public transport card application	See “Application object” in section 4.1.
Co-operate public transport contract / CPTC	See TCCO.
Co-operate public transport purse / CPTP	See TCPU.
Co-operate public transport special ticket / CPTS-x	See TCST-x.
Co-operate public transport ticket / CPTC	See TCTI.
Customer	The person that holds (owns) a travel card. See “Passenger”.
Customer profile	Information on the card that is related to the customer.
Customer transaction	The transaction as experienced by the customer, i.e. from the card is within the active field of the reader until the front system acknowledge the complete transaction. This means a number of read and write commands to the card.
Data element	See section 4.1.
Data element group	See section 4.1.
Data type	See section 4.1.
Directory	See TCDI.
Directory base file	See TCCI.
Directory function	Management function for the organisation of information on a card.
Dual interface card	IC-cards equipped with dual interfaces that give access to the memory of card. One interface is equipped with a galvanic contact and the other interface handles communication by an electromagnetic field.
Event log / CPTL	See TCEL.
Excess fare	A fare that is paid upon a control when a passenger misses a ticket.
Front system	The front system is the part of the ticket system that is placed in the operational environment, like buses, train station, etc. The front system communicates with the back office system and the card.
H	Hexadecimal number

Term or abbreviation	Explanation
IC-card	A card that holds an integrated circuit, e.g. a memory chip or processor and memory together on a chip.
Indivisible transaction	A transaction that always must be fully completed. At the event that the transaction is not, the system, devices or similar returns to the state before the transaction started.
Information owner	On a card, which is used by several public transport authorities the owner (responsible issuer) of a particular information must be well defined. On the RKF travel card there are the following information owners: - Card issuer, which is the public transport authority that has issued the card. The card issuer "owns" the directory and the event log. Normally also the purse is issued in conjunction with the card issuing - the card issuer will in that case also be the owner of the purse. - Application issuer, the public transport authority that has issued a particular application object. The information owner is also the one responsible for that the back office system logs the transactions that shall be logged for the application.
Initialisation	Card transaction that generates and writes a system object to the travel card support layer or an application object to the travel card applications layer.
Inspection	Card transaction that inspects the validity of an application or other sets of data that include validity constraints.
Interchange	Interchange is when the customer changes transportation mode within one journey. The interchange could mean that the customer changes to a new bus or to another vehicle type. Information of valid interchanges should be included in the information of a journey. Interchanges are always included in the validity of the ticket. The ticket can be validated and updated in an interchange transaction.
Interoperability	The extent to which a travel card (including its system objects and application objects) issued by one PTA can be used by other PTAs
Issuer	An authorised user who can write new application objects to the card. The issuer does not have to be the provider of the travel card application.
Issuing	Transaction to the card which generates and writes a ticket or contract to a card.
Journey	A journey with the public transport has an origin, a destination and can include interchanges. A journey can include several journey segments.
Last validation	The last validation is when the ticket is disabled because its validity has finished.

Term or abbreviation	Explanation
MAC	Message Authentication Code. A standardised method by means of symmetrical keys and defined algorithm produce a signature (fingerprint) of the information contents in an application. Is used on the travel card in order to make sure that the information is not compromised.
MAD	Mifare Application Directory. A standard from Philips to define directory function on cards with the Mifare rigid file-system.
NUV-B	Not used in Volume B of this specification
Passenger	A person that uses the travel card for travelling or purchasing. Note several passengers may use the travel card simultaneously for e.g. travelling, but only one is able to hold it. See “Customer”.
Pay method	Pay method is the method of payment for a ticket or a contract. Example: Credit card, cash or electronic purse.
Payment	Payment is when a customer pays for a ticket or a contract with a public transport electronic purse or some other pay method.
PER	Packed Encoding Rules
PIX Proprietary application Identifier eXtension	The purpose of the PIX is to give each PTA or group of PTAs an internal number for type numbering and validation ordering of applications.
Pointer	The pointer gives the address to an specific sector or a specific block on the card.
Protocol	User - card communication rules
PTA	Public Transport Authority. A public organisation that is responsible for mass transportation within a city, region, county or similar area.
Public transport application provider	Provider of public transport applications. The provider is responsible for the public transport application tariffs.
Purchase	A card transaction where the customer buys a ticket or a contract with the TCPU. This transaction decreases the value of the TCPU.
Repurchase	Card transaction that reverses a transaction or parts of it. The repurchase transaction concerns the public transport applications.
RFU	Reserved for Future Use.
RKF	Resekortsföreningen i Norden.
RKF travel card	An IC-card or similar device in compliance with this specification. A RKF travel card contains a number of system objects and application objects

Term or abbreviation	Explanation
Sector	A sector is a predefined file on the card. A card contains at least 16 sectors. A sector has a minimum of 4 blocks, of which 1 block contains the keys necessary to authenticate the use of that sector. This only applies for RKF type 1 cards.
SLTF	Svenska Lokaltrafikföreningen. The Swedish Public Transport Association
System object	See section 4.1.
Tariff	A tariff is an identifier that identifies a set of rules that must be applied to the contract, the ticket or a pay method when they are used.
TCAS Travel card applications status	A system object that controls the update of application objects to ensure indivisible transactions
TCCI Travel card information	A system object that holds information common to all system objects and application objects
TCCO Travel card contract	An optional application object that can include privileges to issue tickets or allow the customer to travel without issuing a ticket
TCCP Travel card customer profile	An optional application object that defines properties of the customer, e.g. default passenger group
TCDB Travel card discount basis	An optional application object that can accumulate information on previous travels to provide the basis for discount fare calculation
TCDI Travel card directory	An object that describes system objects and applications objects of the card
TCEL Travel card event log	An optional application object that can record a limited number of card transactions or other events
TCPU Travel card purse	An optional application object that implements an electronic purse. The TCPU can be used for buying, tickets, contracts or other items
TCRE Travel card reservation	A potential application object implementing a travel reservation. Not part of the specification yet
TCST-x Travel card special ticket	A family of optional application objects that implements specialised tickets or contracts for various purposes
TCTI Travel card ticket	An optional application object that implements an electronic ticket valid for one or more journeys
Transaction log	See TCAS.
Travel card applications layer	A layer of a travel card containing the application objects, e.g. TCPU, TCTI, TCCP
Travel card object	See section 4.1.

Term or abbreviation	Explanation
Travel card support layer	A layer of a travel card supporting the travel card applications layer by system objects, e.g. TCDI, TCAS
Travel card transaction	A travel card transaction is the sum of all elementary actions necessary to complete a desired and controlled change of the card. Examples of travel card transactions are: - Card initialisation - Check-in validation A travel card transaction consists of a number of elementary actions: - Card reads - Data processing - e.g. distance and fare calculation - Card writes
Travel card validation transaction	A validation transaction is a customer or staff initiated transaction in connection with a journey: registration, payment etc. Examples of validation transactions: - Check-in validation - Check-out validation
Unblocking	A transaction that enables an application or a card that previously been blocked. See “Blocking”
Validation	Approval and/or check of the validity of a travel card application with intended journey. The validation can include modifications/updates of contracts and tickets.
Validity	Validity is a number of data elements that describes the conditions under which the ticket, contract, pay method or the card may be used. The validity can refer to time restrictions, geographical restrictions, passenger type restrictions, etc.
Value	A value is a sum defined in a currency, e.g. Swedish kronor. The TCPU has a value.

4.1 Object and data structure of the card - terms

Data and objects on the card are structured the following way:

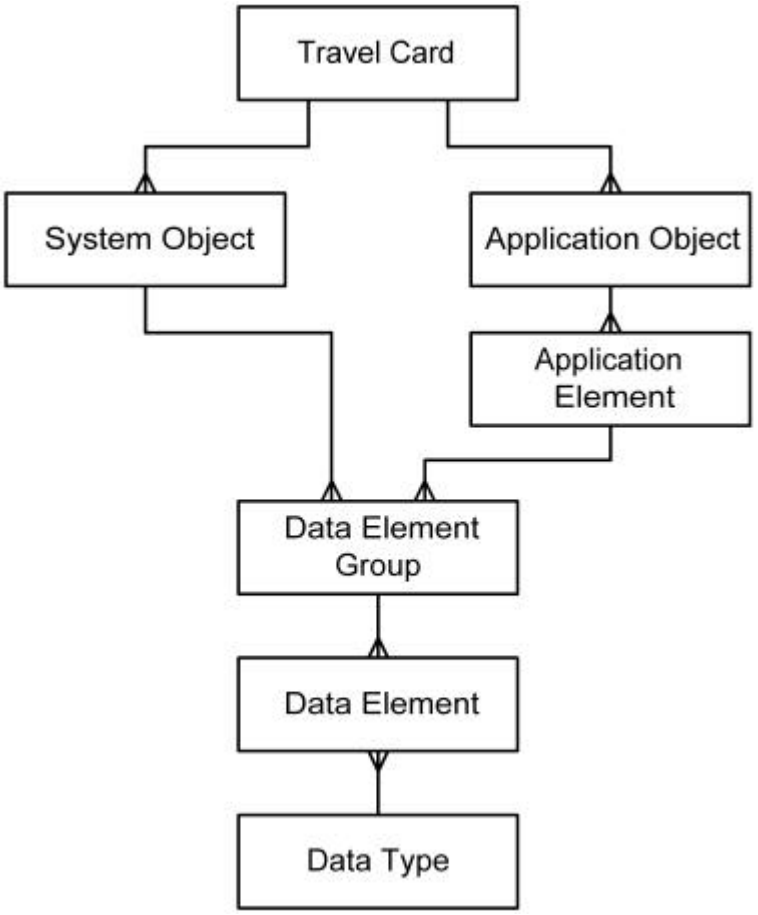

Figure 2 Object and data structure of the card

Travel Card	Is the physical card that holds two main types of objects, System Object and Application Object. The travel card might co-exist with other card application on a multifunction card.
System Object	Is an object that serves Application Objects. A System Object holds information that is global for all Application Objects. It constitutes the structure and basic possibilities of the card. Examples of systems objects are TCAS, TCDI, etc. There may be several System Objects on a Travel Card. All System Objects belong to the Travel Card Support Layer or the Card Issuer Layer.
Application Object	Is an object that holds information concerning the application itself. Examples of Application Objects are TCPU, TCTI, etc. An Application Object consists of one or more Application Elements. E.g. the TCPU consists of a static application element and two dynamic application elements.

	There may be several Application Objects on a travel card. All Application Objects belong to the Travel Card Applications Layer.
Application Element	Any Application object is created by a combination of static and/or dynamic Application Elements. A Static Application Element is created when a new Application Object is introduced on the Travel Card but never updated during the remaining life time of the Application Object. The Dynamic Application Elements are created at the same time as the Static but may be updated frequently during the life time of the Application Object.
Data Element Group	A Data Elemet Group is an object where Data Elements that have similar purposes or tasks are grouped together. Examples of Data Element Groups are: - Period Of Validity - Validity, Distance An Application Element may hold several Data Element Groups.
Data Element	Is the smallest element of the Travel Card. Examples of Data Elements are: - VersionNumber - PassengerClass A Data Element Group may hold several Data Elements.
Data Type	The possible values of a Data Element is defined by a Data Type. Examples of Data Types are: - TimeCompact - Integer 0..1023

5 REFERENCES

The specifications of this volume (Volume B) are referring to the following documents:

Reference	Title
[CEN 1545-1]	Identification card systems surface transport applications, General Data elements.
[CEN 1545-2]	Identification card systems surface transport applications, Transport payment related data elements.
[EMC]	EMC directive Protection requirements and inspection procedures related to apparatus liable to cause electromagnetic disturbances.
[FIPS 113]	National Institute of Standards and Technology (NIST). FIPS Publication 113: Computer Data Authentication. 1985
[ISO 8372]	Information processing - Modes of operation for a 64-bit block cipher algorithm.
[ISO 8731-1]	Banking - Approved algorithms for message authentication.
[ISO/IEC 10116]	Information technology - Security techniques - Modes of operation for an n-bit block cipher.
[ISO/IEC 14443-1]	Identification cards - Contactless integrated circuit cards - Proximity cards - physical characteristics
[ISO/IEC 14443-2]	Identification cards - Contactless integrated circuit cards - Proximity cards - Radio frequency power and signal interface
[ISO/IEC 7816-1]	Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics.
[ISO/IEC 7816-3]	Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols.
[ISO/IEC 7816-4]	Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry command for interchange.
[ISO/IEC 7816-5]	Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers.
[ISO/IEC 7816-6]	Identification cards - Integrated circuit(s) cards with contacts - Part 6: Inter-industry data elements.
[ISO/IEC 9797]	Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm.
[ISO/IEC 9798-2]	Information technology -- Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms.
[RKF-0017]	RKF Travel Card – Volume B Introduction
[RKF-0018]	Setting of keys and application identifiers - Edition A
[RKF-0019]	Setting of keys and application identifiers - Edition B

Reference	Title
[RKF-0020]	RKF Travel Card Requirement specification
[RKF-0021]	RKF Travel Card Technical Requirement Specification
[RKF-0022]	RKF Travel Card Implementation Specification Type 1
[RKF-0023]	RKF Travel Card Implementation Specification Details Type 1
[RKF-0024]	RKF Travel Card Implementation Guide Type 1
[SLTF specification]	See section 3.

A reference to e.g. “Identification cards - Contactless integrated circuit cards - Proximity cards - physical characteristics” of the above documents is made “[ISO/IEC 14443-1]”.

6 MAINTENANCE OF THE DOCUMENTATION SET UP

Resekortsföreningen i Norden maintains the standard that this documentation set up represent. The board of the association initiates any change of the standard. A change may be initiated in two ways:

- By a request from a member of the association.
- By a change request issued by an interested party, such as a public transport company that is not a member of the association or a supplier of ticketing equipment.

A change request should be forwarded to the following address:

Resekortsföreningen i Norden Ekonomisk Förening
Box 5193
SE-121 18 STOCKHOLM-GLOBEN
Sweden

A change request forwarded to Resekortsföreningen should at least hold the following information:

Date	The date when the change request is issued.
Issued by	Name and address of the organisation that issued the change request.
Liaison person	Name of whom to get in contact with.
Change	The actual change that is requested.
Reason	Reason for the request.
Reference	Reference to specifications.