Prepared by	Document id	Version	Document date
	RKF-0021	2.00	22 January 2002

RKF Travel Card
Technical Requirement Specification

CONTENTS

1   INTRODUCTION

1.1   Scope

This document specifies requirements for selected IC-card technologies for the RKF travel card, thereby supplementing the card technology independent part of the RKF Requirement Specification [RKF-0020]

Together with the general requirements in [RKF-0020], this document outlines the requirements for each defined card technology. For each relevant technology a description of how a possible implementation should be handled is given in three separate documents, namely the Implementation Specification, the Implementation Specification Details, and the Implementation Guide.

Both the Requirement Specification and this document refer to the three above mentioned type specific documents for detailed information beyond the overall requirements common for all types.

This specification defines one type of card technology:

RKF Type CL-1: Contactless IC-cards compatible with Mifare® Standard (1 kB, type A card according to [ISO/IEC 14443-1 and -2], MF1 IC S50 chip).

The implementation of the RKF travel card specification using the Type CL-1 card technology is described in the three documents [RKF-0022], [RKF-0023], and [RKF-0024].

Future volumes of this specification are expected to comprise additional card technologies, either cards with contactless interface (Type CL-x), cards with contact interface (Type CO-x), or dual interface cards (Type DI-x).

1.2   Reader's Guide

Chapter 2 gives an overview of the RKF travel card.

Chapter 3 defines technical requirements on the technical layers.

A knowledge of the section 'Standards in Relation to These Specifications' of [RKF-0017] is assumed.

The requirements that are defined in this document are divided in three levels: mandatory requirements ("must", "shall"), recommended requirements ("should"), and optional requirements ("could", "may"). These levels of requirements are described in [RKF-0017] (section 'Levels of Requirements').

2   OVERVIEW OF THE RKF TRAVEL CARD

2.1   General

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 techniques (e.g. technologies with or without contacts) and the RKF travel card application objects (e.g. purse, ticket, and contract).

A contactless card may have other shapes than a traditional IC-card as long as the transmission protocol is correct. A contactless card might for instance have the shape of a watch or a key ring.

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 'RKF travel card system overview' (see below) shows the layers and their relations.

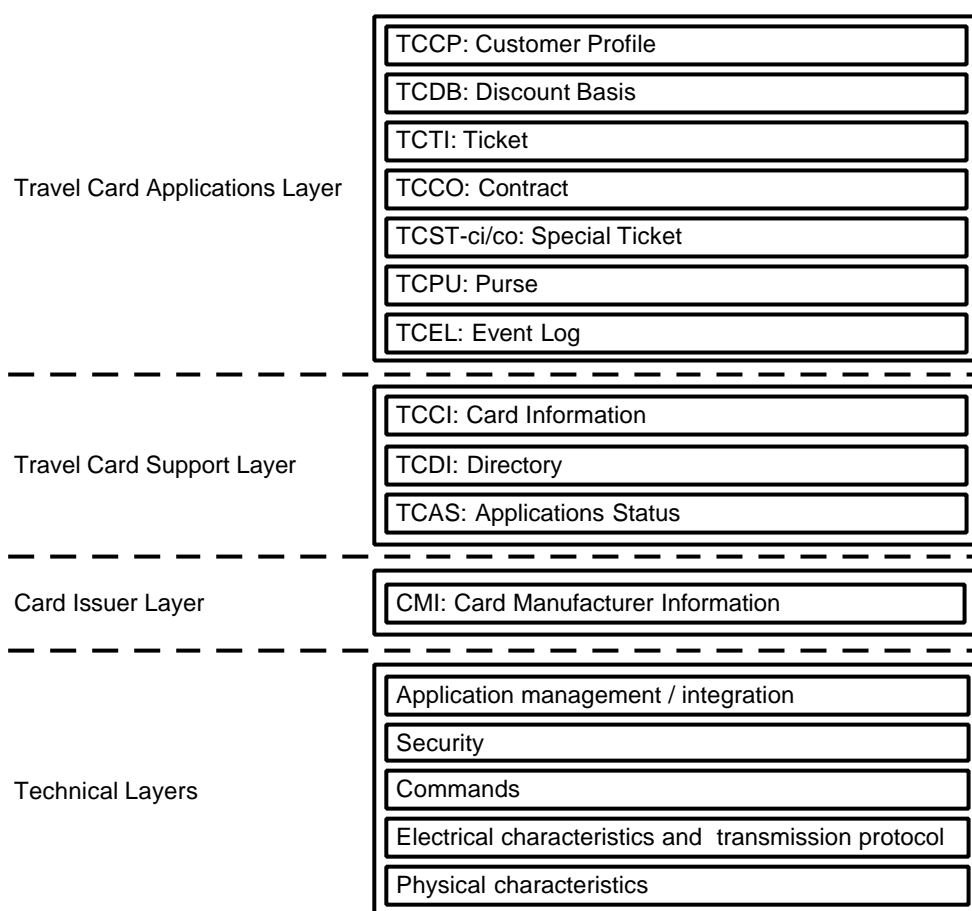|	
Travel Card Applications Layer	TCCP: Customer Profile
	TCDB: Discount Basis
	TCTI: Ticket
	TCCO: Contract
	TCST-ci/co: Special Ticket
	TCPU: Purse
	TCEL: Event Log
Travel Card Support Layer	TCCI: Card Information
	TCDI: Directory
	TCAS: Applications Status
Card Issuer Layer	CMI: Card Manufacturer Information
Technical Layers	Application management / integration
	Security
	Commands
	Electrical characteristics and transmission protocol
	Physical characteristics

Figure 1: RKF travel card system overview

The document [RKF-0020] specifies relevant requirements on the layers:

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

The layers specified in this document are the technical layers.

- Application management/integration
- Security
- Commands
- Electronic signals and transmission protocols
- Physical characteristics

2.2   Application Management/Integration

The Application management/integration layer is the technical layer that defines the card structure on which an implementation of RKF travel card is based.

2.3   Security

The Security layer specifies the demands for security on cards such as access rights, authentication, encryption, cryptography etc.

2.4   Commands

The Command layer specifies the command structure that is implemented on a card.

2.5   Electronic Signals and Transmission Protocols

The Electronic signals and transmission protocol layer specifies which transmission protocols and electronic signals that are used for the card technology in question.

2.6   Physical Characteristics

The Physical characteristic layer specifies the cards physical size and environmental requirements on card, specifying both manufacture materials and operation environment.

---

3 REQUIREMENTS OF THE TECHNICAL LAYERS

The technical layers define the technical demands on the RKF travel card. The definition concerns contactless cards, contact cards, and dual interface cards.

The requirements of each layer is divided into a subsection describing common requirements for all card technologies and subsections describing requirements specific to each card technology.

3.1 Application Management/Integration

3.1.1 Common Requirements

The Application management/integration layer is the layer that defines the card structure of the RKF travel card on a specific physical card or on a card equipped with a specific physical chip.

Requirements:

- The card must have an addressable memory.

- It must be possible to address the memory on at least file level or similar level.

- It must be possible to write and read from different files (or similar structures) on the card.

- For dual interface cards, the contactless interface and the contact interface must give access to one common memory and one shared microprocessor.

3.1.2 RKF Type CL-1 Requirements

The Application management/integration layer is a part of the Mifare Standard proprietary protocol for interchanging data between a CAD and a card (as described in [M01040]) or compatible protocol.

The card structure is the Mifare sector/block structure, which is a 1 kB memory structure divided into 16 sectors. Each sector has 4 blocks of 16 B. The last block of each sector is reserved for controlling access authentication.

The card is based on a MF1 IC S50 chip.

The common requirements are met.

3.2 Security

3.2.1 Common Requirements

Access rights shall be possible to activate at least on file level or similar level.

Access rights shall be possible to activate/deactivate for write, read, and possible functions done by the card.

It should be possible to define authorisation to specific files (or similar units) on the card.

The card should have support for authentication by challenge and response.

The communication between card and card-reader should have possibilities to be encrypted.

The card should have functions to maintain data integrity.

The card should have functions to maintain transaction integrity.

3.2.2 RKF Type CL-1 Requirements

The Security layer is a part of the Mifare Standard proprietary protocol for interchanging data between a CAD and a card (as described in [M01040]) or compatible protocol.

The common requirements are met.

Note, that the functions to maintain data integrity and transaction integrity are a part of the Travel card support layer.

3.3 Commands

3.3.1 Common Requirements

The Commands layer defines the commands for accessing the contents of the card. The commands must support the card structure and the security mechanisms.

The command set can for example be in accordance with [ISO/IEC 7816-4].

3.3.2 RKF Type CL-1 Requirements

The Commands layer is a part of the Mifare Standard proprietary protocol for interchanging data between a CAD and a card (as described in [M01040]) or compatible protocol.

The commands support access to the Mifare sector/block structure.

The common requirements are met.

3.4 Electronic Signals and Transmission Protocols

3.4.1 Common Requirements

This layer must specify the electronic signals and the transmission protocol.

The card and the CAD must follow the EMC-directive [EMC].

3.4.2   RKF Type CL-1 Requirements

This layer is a part of the Mifare Standard proprietary protocol for interchanging data between a CAD and a card (as described in [M01040]) or compatible protocol.

Furthermore the card must be in compliance with type A cards as defined in [ISO/IEC 14443-2].

Cards should have full functionality up to a range of 10 cm from the CAD.

The common requirements are met by the card. This specification cannot ensure, that the requirements of the CAD are fulfilled.

3.5   **Physical Characteristics**

3.5.1   Common Requirements

The physical card on which the RKF travel card is implemented should be in accordance with [ISO/IEC 7816-1].

Contactless cards should also follow the [ISO/IEC 14443-1]. However, contactless cards shall not necessarily have the shape of traditional IC-cards.

Because of environmental influence, the card should be manufactured in other materials than PVC, preferably ABS, polycarbonate, or any other materiel with little environmental influence.

It shall be possible to store information on the card for at least 10 years.

It shall be possible to do at least 100000 operations to the card during its life-cycle.

No technical maintenance on the card is allowed.

The card should be easy for the user to clean externally.

3.5.2   RKF Type CL-1 Requirements

The card must be in accordance with [ISO/IEC 14443-1]. If the travel card does not have the shape of a traditional IC-card, the required dimensions etc. are irrelevant.