3 Technological Development

3.1 Preliminary remarks

The Recommendations for Action 2000 (hereafter referred to as RA2000) described in detail the necessary components, on both the hardware and software sides, for the systems engineering platform of an eTicketing system. The description of the semiconductors, the antenna technologies, the card materials and the operating systems represented the state of the technology at the end of 1999/ beginning of 2000.

The purpose of this issue of the Recommendations for Action is to
1. update the technological description
2. consider new developments that could not be thoroughly addressed when RA2000 was created
3. place these technologies in the context of a ticketing system.

Chapter 3.2 picks up where the developmental trends in RA2000 left off.
- What advances have taken place in the card technologies?
- What has changed in terms of the chips (the semiconductor ICs?)

In addition to the application of the contactless proximity and vicinity transmission techniques for electronic ticketing, it is essential to investigate a range of other such techniques, such as mobile telephone networks and Bluetooth. This topic is dealt with in Chapter 3.3.

The application of new transmission technologies in the ticketing environment necessitates certain new customer media, or enables the employment of media currently used in other domains (e.g. the mobile telephone) in electronic ticketing (Chapter 3.4).

If we consider automatic fare determination as Step 3 in the development of an electronic fare management system, new transmission techniques also facilitate new solutions. The focus up to now has been on active check-in/ check-out. With the help of other transmission techniques and as a result of new customer media, solutions would be conceivable in which any activity by the customer at/in the vehicle or at the gate could be dispensed with. Chapter 3.5 shows how the vision of simply "boarding and riding" could be realized technically.

Because a ticketing system appears not only at the interface between customer medium and terminal, the operation of the background system is equally important. Chapter 3.8 deals with the design of such a background system.
If the interoperability of a chip card application is not to be limited to the regional level, but rather it is to be accepted nationally or even internationally, standardization of chip technique and chip application is indispensable.

Chapter 3.9 addresses the topic of interoperability and illustrates the latest state of the art in standardization efforts at the international level.

3.2 Further development of chip card technology

The developmental trends for chip cards cited in RA2000 will first be updated.

3.2.1 Card physics

Today's user has access to a wide range of contactless chip cards. In selecting a card, it is recommended to consider a few key aspects of card technology, in order to choose the most suitable card for the respective application.

Today's standard contactless card is nothing but a card with a memory chip. Cards with contactless microprocessor chips have not caught on up to now.

For additional applications, however, the simple contactless memory card is increasingly being equipped with a second independent contact-based chip; this is known as a "hybrid card."

Outfitted with a novel microprocessor, the dual interface card is currently being introduced by a variety of manufacturers. Such cards feature contactless and contact-based access to a common processor.

In a chip card, the chip is usually located on a module. In contactless cards, this module is connected with the antenna; together they form the transponder. However, card structures have recently been introduced in which flip chip technology is implemented, making a module unnecessary. Modules for dual interface cards have been developed that allow the customary contact with card readers, and at the same time feature a connection for the antenna on the reverse.

A number of manufacturers have developed new procedures in the past few years for realizing antennae in chip cards, based on the wound coil. The etched or wired copper coil is the standard antenna today. The recently introduced printed coil antenna may contribute to further optimizing the manufacturing process.

Technical comparison of card materials

FIG. 3.2.1.1

Characteristic	PVC	ABS	PET	PC
Temperature stability Physical durability	good	good	good	excellent
Suitable for contactless cards	yes	under certain conditions	under certain conditions	no
Personalization	laser engraving /embossing thermal printing	laser/embossing	laser/embossing thermal printing	laser thermal printing
Service life	approx. 4 yrs.	approx. 4 yrs.	approx. 4 yrs.	5+ yrs.
Printability	excellent	excellent	good	good
Availability	certain	currently uncertain	uncertain	partially uncertain

The card bodies of the vast majority of today's contactless cards consist of PVC (polyvinyl chloride). Other materials such as PET (polyethylene terephthalate) and ABS (acrylonitrile-butadiene-styrene) are becoming more popular.

Ecological comparison of card materials

FIG. 3.2.1.2

Characteristic	PVC	ABS	PET	PC
Recycling	realized, possible together with ABS	realized, possible together with PVC	not possible	not realized
Fire behavior	self-extinguishing	flammable heavily sooting	flammable	flammable
Disposal, waste incinerator	accepted	accepted	unproblematic	accepted
Uncontrolled incineration	highly problematic	problematic	problematic	problematic
Fabrication	chlorine chemistry	no chlorine	no chlorine	chlorine chemistry

In the case of the durable, premium PC (polycarbonate) material, there are still a number of technological obstacles to overcome in laminating the antennae, before market penetration can be achieved (see Figs. 3.2.1.1, 3.2.1.2).

In addition to modifying the surface through print processes (typically sheet-fed or single-card printing), most of the other familiar card features can also be implemented today on a contactless card.

These include
- the application of a magnetic strip
- the application of a hologram
- the application of a signature strip or a kinegram (special type of surface-relief hologram)

The realization of characteristics typical for credit cards, such as
- embossing
- laser engraving
- photo personalization
- transparent overlays (security for premium cards) is likewise possible.

Note:
With the help of an electronic shell, contact chip cards can also be used in a contactless manner.

3.2.1.1 Optical security features of chip cards

Due to the great value of monthly or yearly cards, it also makes sense to equip the card bodies with security features, in addition to the security of the chips.

The following printing capabilities ensure comprehensive security against counterfeiting:

Visible features	Non-visible features
Guilloche printing	UV-visible inks
Microprinting	IR-visible inks
Fine line printing	Anti-copy colors
Iris printing	Interference colors
	Thermochromic inks

Although the **visible features** can easily be recognized with the naked eye, they are very difficult to copy. Forgeries can be easily identified.

The **non-visible features** can only be recognized under special technical conditions, for example with a flashlight whose source only emits light in a limited range of wavelengths (counterfeit banknote detectors).

A hologram on the card is another security feature; it meets the highest security standards, as it is practically unforgeable.

Tactile features (lines) can be embossed on the card and felt by touch.

Through **laser engraving, ghost images** (e.g. photos) can be engraved, which are recognizable from several viewing angles.

3.2.2 Semiconductor ICs

Overview/selection of contactless chip card memory ICs: PROXIMITY (as of 03/2003)

FIG. 3.2.2.1

Chip designation	Mifare Standard 1k	Mifare Standard 4k	Mifare UltraLight	Mifare DESFire	Mifare SLE 44R35S/T	Mifare SLE 66R35	my-d prox SLE 55R01
Manufacturer	Philips	Philips	Philips	Philips	Infineon	Infineon	Infineon
Standard ISO/IEC	14443-A	14443-A	14443-A 512 bits	14443-A (complete), 4 kB	14443-A	14443-A	14443-A
Memory (EEPROM)	1 kB	4 kB	(32 bits OTP)	(with MMU)	1 kB	1 kB	160 Bytes
Encryption	Crypto-1	Crypto-1	via terminal	3DES	Crypto-1	Crypto-1	my-d
Multi-application	yes	yes	possible	yes	yes	yes	yes
Anti-collision	yes	yes	yes	yes	yes	yes	yes
Speed (kBaud)	106	106	106	106-212-424	106	106	106
Availability	yes	yes	yes	yes	yes	yes	yes
Projects	> 10.000	new, a few	new, a few	new, a few	> 100	new, a few	> 10

Chip designation	my-d prox SLE 55R04	my-d prox SLE 55R08	my-d prox SLE 55R16	M 3510x	M 37009	SR176	SRIX4K
Manufacturer	Infineon	Infineon	Infineon	ST	ST	ST	ST
Standard ISO/IEC	14443-A	14443-A	14443-A	14443-B	14443-B	14443-B 176 bit	14443-B 4 kB
Memory (EEPROM)	770 Bytes	1280 Bytes	2560 Bytes	2048 bit	512 bit	+64 bit UID	+64 bit UID
Encryption	my-d	my-d	my-d	via terminal	authenticate	via terminal	anti-clone
Multi-application	yes	yes	yes	yes	yes	yes	yes
Anti-collision	yes	yes	yes	yes	yes	yes	yes
Speed (kBaud)	106	106	106	106	106	106	106
Availability	yes	yes	yes	yes	yes	yes	yes
Projects	> 50	> 10	> 10	a few	new	new	new

Chip designation	LEGIC ATC1024-MP	LEGIC ATC2048-MP
Manufacturer	Kaba	Kaba
Standard ISO/IEC	14443-A	14443-A
Memory (EEPROM)	1024 Bytes	2048 Bytes
Encryption	LEGIC	LEGIC
Multi-application	yes, max. 127	yes, max. 127
Anti-collision	yes	yes
Speed (kBaud)	106	106
Availability	4th quart. 2003	4th quart. 2003
Projects	new	new

Definitions:

OTP = one-time programmable
MMU = memory management unit
1 kB = 1024 Bytes = 8192 bits
Crypto-1 = original encryption protocol for Mifare interface
my-d = encryption protocol for the my-d interface (key length 64 bit)
UID = unique identification number

Overview/selection of contactless chip card memory ICs: VICINITY (as of 03/2003)

FIG. 3.2.2.2

Chip designation	LRI 512	my-d vic SRF 55V02P	my-d vic SRF 55V02S	my-d vic SRF 55V10P	my-d vic SRF 55V10S	I-code 1
Manufacturer	ST	Infineon	Infineon	Infineon	Infineon	Philips
Standard ISO/IEC	15693 512 bit	15693	15693	15693	15693	15693
Memory (EEPROM)	+64 bit UID	2500 bit	2500 bit	10000 bit	10000 bit	512 bit
Encryption	via terminal	via terminal	my-d	via terminal	my-d	via terminal
Multi-application	yes	yes	yes	yes	yes	possible
Anti-collision	yes	yes	yes	yes	yes	yes
Speed (kBaud)	26	26	26	26	26	26
Availability	yes	yes	2nd quart. 2003	yes	2nd quart.2003	yes
Projects	new	new, a few		new, a few		> 50

Chip designation	I-code SLI	I-code HSL	LEGIC ATC256-MV	LEGIC ATC1024-MV	LEGIC MIM 256	LEGIC MIM 1024
Manufacturer	Philips	Philips	Kaba	Kaba	Kaba	Kaba
Standard ISO/IEC	15693	18000 WD	15693	15693	nein	nein
Memory (EEPROM)	1024 bit	2048 bit	256 Bytes	1024 Bytes	256 Bytes	1024 Bytes
Encryption	via terminal	via terminal	LEGIC	LEGIC	LEGIC	LEGIC
Multi-application	possible	possible	yes, max. 30	yes, max. 127	yes, max. 30	yes, max. 127
Anti-collision	yes	yes	yes	yes	detection	detection
Speed (kBaud)	26-52	max. 40	26	26	12	12
Availability	yes	3rd quart. 2003	4th quart. 2003	2nd quart. 2003	yes	yes
Projects	> 50	new	new	new	> 20	a few

Overview/selection of dual-interface chips (as of 03/2003)

FIG. 3.2.2.3

Chip designation	Mifare ProX	Smart MX P5 SD 016/032	Smart MX P5 CD 016/032/064	Smart MX P5 CT 064 triple interface	my-C SLE 66CL160S	my-C SLE 66CLX 320P	my-C SLE 66CL80P
Manufacturer	Philips 14443-A	Philips 14443-A	Philips 14443-A	Philips 14443-A	Infineon 14443-A/B	Infineon 14443-A/B	Infineon 14443-A/B
Standard ISO/IEC	7816	7816	7816	7816 + USB1.1	7816	7816	7816
Memory (EEPROM)	4/8/16 kB 3DES/RSA/ECC	16/32 kB	16/32/64 kB 3DES/RSA/ECC	8/16/32/64 kB 3DES/RSA/ECC	16 kB	32 kB 3DES/ECC/RSA	8 kB
Encryption	AES/Crypto-1	3DES/Crypto-1	AES/Crypto-1	AES/Crypto-1	3DES/ECC	AES	3DES
Multi-application	yes	yes	yes	yes	yes	yes	yes
Anti-collision	yes	yes	yes	yes	yes	yes	yes
Speed (kBaud)	106-212-424-848	106-212-424-848	106-212-424-848	106-212-424-848	106	424	424
Availability	yes	yes	yes	yes	yes	1st quart. 2003	2nd quart. 2003
Projects	> 25	new	new	new	> 20	new	new

Chip designation	ST16Rxx	ST19RF08	ST19XR08	ST19XR34
Manufacturer	ST 14443-B	ST 14443-B	ST 14443-B	ST 14443-B
Standard ISO/IEC	7816	7816	7816	7816
Memory (EEPROM)	0.5 bis 8 kB	8 kB	8 kB	34 kB
Encryption	DES	3DES	3DES	3DES/RSA/ECC
Multi-application	yes	yes	yes	yes
Anti-collision	yes	yes	yes	yes
Speed (kBaud)	424	424	424	424
Availability	yes	yes	yes	yes
Projects	a few	a few	new	new

Definitions:

OTP =	one-time programmable
MMU =	memory management unit
1 kB =	1024 Bytes = 8192 bits
Crypto-1 =	original encryption protocol for Mifare interface
my-d =	encryption protocol for the my-d interface (key length 64 bit)
UID =	unique identification number

3.2.3 Chip software

There are a variety of open operating systems (JAVA, MULTOS) as well as closed (proprietary) ones available that can accommodate the requirements of the VDV core application or electronic ticketing.

3.3 Innovative, contactless transmission techniques

For the sake of completeness, the proximity and vicinity transmission techniques for chip cards will again be described and compared with one another. But in designing a ticketing system, one should not a priori limit oneself exclusively to these techniques.

It is just as important to take other developments into account and analyze their applicability in the system design. In the end, the decision for or against such an innovate technology will be made through the kind of business processes and their functionalities that the respective system should provide.

Overview of contactless transmission techniques

FIG. 3.3 In this overview, all entries have been reduced to the most basic information

	Proximity	Vicinity	Wide-Range	GSM UMTS	Bluetooth	IrDA
Frequency	13.56 MHz	125 kHz 13.56 MHz	400 MHz to 5.6 GHz	900 MHz to 2 GHz	2.45 GHz	10^{13} to 10^{14} Hz
Transmission type	inductive coupling	inductive coupling	wireless (radio)	wireless (radio)	wireless (radio)	infrared
Transmission rate	106 to 848 KBit	1.6 KBit to 26.5 KBit	1MBit	10 KBit to 2 MBit	1 MBit	9.6 KBit 4 MBit
Connection type	point-to-multipoint	P-to-MP	P-to-MP	P-to-MP	P-to-MP	P-to-P
Anti-collision	yes	yes	yes	yes	yes	no
Distance	< 0,12 m	< 1 m	< 30 m	Global	< 10 m	< 2 m line of sight

3.3.1 Proximity (ISO/IEC14443)

The ISO/IEC 14443 standard has fulfilled the great expectations of strengthening the market for contactless chip cards. This standard, developed under German leadership by the JTC1's working group SC17/WG8, describes the physical and data systems characteristics of the transmission route between a reader and the chip cards, which are designated "proximity integrated circuit cards (PICC)" in this standard.

The name "proximity" reflects the intended transmission range of approximately 10 cm associated with these chip cards. The PICCs are differentiated into types A and B, which differ with respect to their modulation procedures.

The card reader provides the contactless chip card with energy and a system clock. Data transmission from the reader to the contactless chip card occurs through amplitude shift keying (ASK), i.e. by switching a high-frequency magnetic field on and off (Type A = ASK 100%/Type B = ASK 10%).

3.3.2 Vicinity (ISO/IEC15693)

Another standard, ISO/IEC15693 (likewise developed by SC17/WG8) uses the same logic as proximity to define the characteristics of contactless chip cards, with a range of up to 1 m.

These cards are referred to in the standard as "vicinity integrated circuit cards (VICC)," to indicate the larger range.

The standard is widely used in access systems today.

3.3.3 Comparison of proximity and vicinity

The only common feature between the two PICC types **A** and **B** and VICC is the uniform transmission frequency of the reader at 13.56 MHz. This makes it an ISM (industry-science-medicine) frequency, available in almost every country in the world for low-power wireless applications.

Both transmission types have their own standard, but aren't compatible with one another in application. If a single reader is to process data media according to both standards, the technologies for both must be integrated into the terminal. Such terminals are already available today.

It is also true for both systems that they do not necessarily have to be located on plastic cards, but can also be integrated into customer-specific storage media, such as keychains, watches, etc. Recently, it has also been possible to incorporate such storage media, including the reception/transmission antennae, in paper tags or cards, which means reduced manufacturing costs but shorter service life. Further application fields will certainly develop.

3.3.4 Wide-Range

The aim of this technology is to achieve a range as great as possible (> 1 m) within non-reserved frequencies (i.e. cannot interfere with or overlap police radio) using approved transmission powers (so that hazards to health are excluded).

Wide range systems usually use active transponders. These are comprised of a variety of electronic components, an antenna, and a power supply; for this reason, active transponders are located in sturdy plastic housings.

Because of the integrated voltage supply, the transponder can always be activated by an external signal. After the data has been exchanged between the card and the detection unit, the transponder reverts to an energy-saving mode after a certain period of time.

Active transponders are available primarily in ultra-high frequency domains. The actual working ranges may vary, depending on system design and manufacturer.

3.3.5 Mobile telephone network

Increasing numbers of public transportation users in Germany already possess a GSM mobile telephone and thus a potential, secure, personal medium for transmitting and storing a ticket.

eTicketing applications can already be depicted in mobile telephones through the GSM toolbox. Problem areas still include inadequate roaming specifications, the secure depiction of tickets in mobile telephones, and agreements regarding secure payment transactions (because it must be guaranteed that the eTicketing procedure is supported throughout the area by all mobile providers, as well as integrating all credit institutes and banks).

Corresponding procedures are now being specified and should be available in the near future.

Appropriate interfaces could also enable the future use of mobile telephones in in/out systems (CICO, BIBO).

The current mobile network standard (GSM), with transmission rates of 9.6 Kbit/s (up to now) or 14.4 Kbit/s and the existing encryption, is already sufficient for eTicketing applications.

Newer procedures such as GPRS (General Packet Radio Service) and UMTS (Universal Mobile Telecommunication System) allow even faster data exchange. They might be able to eliminate current bottlenecks due to low network capacities at busy transportation stations. The choice of transmission procedure has no influence on the depiction of the eTicket.

3.3.6 Bluetooth

Bluetooth is a short-range wireless radio standard that enables communication between different devices.

The conceptual design:
A small, simple wireless radio module that requires little energy, provides integrated security mechanisms and is inexpensive to manufacture, enabling it to be employed in a broad range of electronic devices. It is already integrated into mobile telephones and PDAs today.

The power consumption is low (0.3 mA in standby mode, maximum 300 mA). Bluetooth currently allows the transmission of data throughputs of 1Mbit/s across typical ranges of 10 cm to 10 m. The range can be extended to more than 100 m if the transmission power is increased.

Bluetooth uses the global industrial-scientific-medical (ISM) frequency band at 2.45 GHz.

3.3.7 IrDA (infrared data association)

IrDA is a point-to-point connection that transmits data at a rate of 1Mbit/s over a distance of at least 1 m. The standard has already been integrated worldwide in numerous PDAs, mobile telephones, notebooks, peripherals, and network systems. In the long run, however, IrDA is being displaced by Bluetooth.

The contactless transmission of data via Bluetooth and IrDA is mentioned here for the sake of completeness; from today's perspective, neither procedure is feasible for use in automated fare determination systems, for a variety of reasons.

However, the transmission of pre-selected tickets to a PDA or mobile from a stationary PC (desktop or notebook) via the internet would be conceivable.

3.4 New customer media

Chip cards as passive media (no batteries)

FIG. 3.4.1

Contact card
Card with a memory or microprocessor chip with no contactless function. This makes it suitable only for contact-type ticketing procedures.

Contactless plastic card
Re-loadable card, especially suited to multiple tickets/use of supplementary contactless applications; a re-writable coating (TRW film) is applied for temporary writing (this additional function is possible on all plastic cards).

Contactless paper ticket
Economical; can be written to with a standard printer; re-loadable, less durable than a plastic card; as a single ticket, day pass, or multiple ticket for tourists and occasional users.

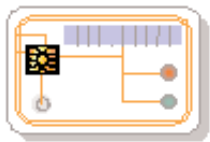
Hybrid card
In addition to the contactless chip, this card features a second, completely separate contact-type chip for additional applications, e.g. an electronic wallet, which can only be implemented in contact-based applications

Chip cards as passive (no batteries) **or active** (battery-operated) **media**

FIG. 3.4.2

Dual interface card
Functions similarly to the hybrid card but with a single chip that can be activated in both a contactless and contact manner (e.g. for eWallet).

Triple-interface card
Functions like the dual interface card; in addition to contactless and contact interfaces, the chip features a USB interface (e.g. for simple communication via a PC's USB interface).



Micro-system card
A card or compact module equipped with different technical features, depending on requirements (e.g. display, function buttons, sender/receiver, battery, solar cell). This technology is already available today as a prototype, but is significantly thicker than specified by the ISO standard.

Great efforts are currently being made to realize such a hybrid system in ISO format, to specify standards, and to develop economical manufacturing processes.

Other forms of passive and active media

FIG. 3.4.3

Transponder shell

The shell is typically equipped with a power source (solar or battery), a display, and one or more function buttons.

It allows a contact-type card to additionally function as a contactless card. The card is placed in the shell for contactless use, but it must be removed again for contact-type applications.

Tags

Tags are active or passive media available in a variety of forms, such as keychains, watches, wristbands, etc. The form can be adjusted to its function or the desires of the user, for instance by installing the transponder in ski gloves.

Mobile telephone

The mobile telephone is enjoying ever-increasing acceptance, and offers the technical opportunities of generating and presenting a ticket independent of time or location. However, the necessary standards and agreements regarding secure ticketing and payment function are not yet in place.

PDA

A PDA can also be employed as a carrier medium for electronic tickets. The typical IrDA interface, however, is not optimally suited to contactless transmission in the public transportation environment.

Overview and availability of customer media

FIG. 3.4.4

Media	Size Format ISO 7810	Transmission procedure Contact ISO 7816	Proximity ISO 14443	Vicinity ISO 15693	Wide Range	GSM-UMTS	IrDA	Blue-tooth
Passive (power supply from the terminal within the corresponding range)								
Contact-type card	●	●	▲	▲	▲	▲	▲	▲
Dual interface card	●	●	●	■	▲	▲	▲	▲
Hybrid card	●	●	●	●	▲	▲	▲	▲
Contactless card	●	▲	●	●	▲	▲	▲	▲
Contactless paper ticket	▲*	▲	●	●	▲	▲	▲	▲
Tag	▲	▲	●	●	▲	▲	▲	▲
Triple interface card	●	●	●	▲	▲	▲	▲	▲
Aktive (with own power supply)								
Micro-system card	○	▲	○	○	■	▲	▲	▲
Transponder shell	▲	▲	▲	▲	○	▲	○	■
Mobile telephone	▲	▲	▲	▲	▲	●	●	●
PDA	▲	▲	▲	▲	▲	●	●	●
Tag	▲	▲	▲	▲	●	▲	●	●

* Thickness not ISO-compliant

Legend, according to availability ● = immediate ○ = middle-term ■ = long-term ▲ = not available

3.5 Techniques for automatic fare determination procedures

Overview of techniques for automatic fare determination procedures

FIG. 3.5 In this overview, all entries have been reduced to the most basic information.

Procedure	Standardized media	Distance	Arrangement of terminals	Active action
Check-in / check-out (CiCo)	ISO/IEC14443	< 0.12 m	Terminal at each vehicle entrance or at a gate	yes
Walk-in / walk-out (WiWo)	ISO/IEC15693	< 1 m	Antennae frame at each entrance or at a gate	no
Be-in / Be-out (BiBo)	none	< 30	Up to 3 in each vehicle	no
	This technology is in the test phase, but not yet currently available for use in fare management			
Combinations	none		mixed	depending on combination

3.5.1 Check-in / check-out (CiCo)

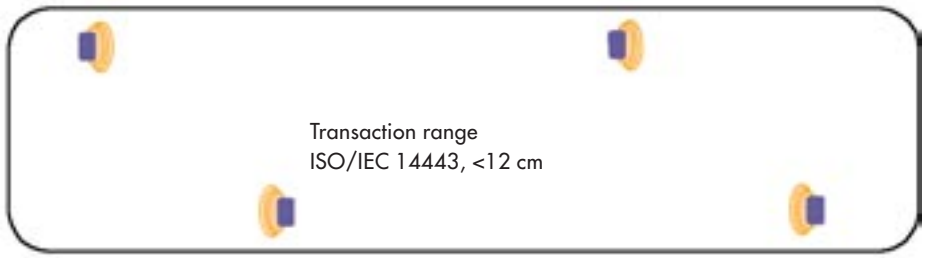
Upon entering the entrance area or the means of transportation, the customer checks in at a corresponding terminal (Ci), and checks out in the same manner upon exiting (Co).

The data stored on the card upon checking in to the public transportation application serves the customer and the transportation company's inspectors as proof of possessing a valid ticket.

The customer, however, is forced to carry out two actions (similar to canceling a conventional ticket today).

Arrangement of terminals in the vehicle's entrance area

FIG. 3.5.1



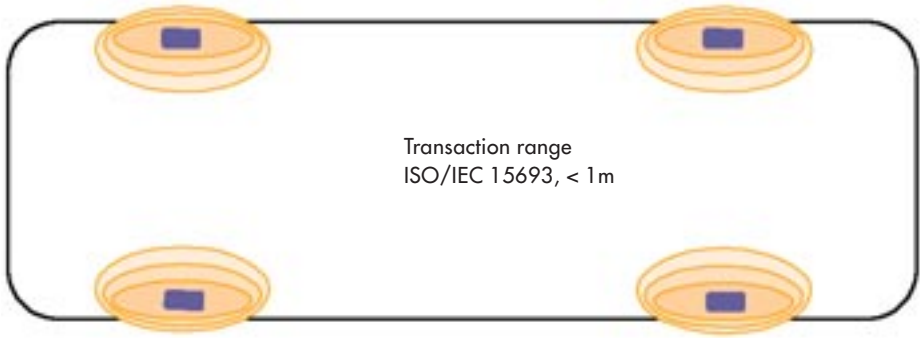
3.5.2 Walk-in / walk-out (WiWo)

This procedure allows the automatic detection of customer movement upon boarding (Wi) and exiting (Wo) the means of transportation. Registration occurs without any check-in or check-out activity on the part of the customer.

This allows rapid processing, which is especially positive when many passengers must be processed. Every movement of the customer, even in the case of transfers, is registered exactly. This makes optimized fare determination possible.

Arrangement of terminals in the vehicle's entrance area

FIG. 3.5.2



3.5.3 Be-in / Be-out (BiBo)

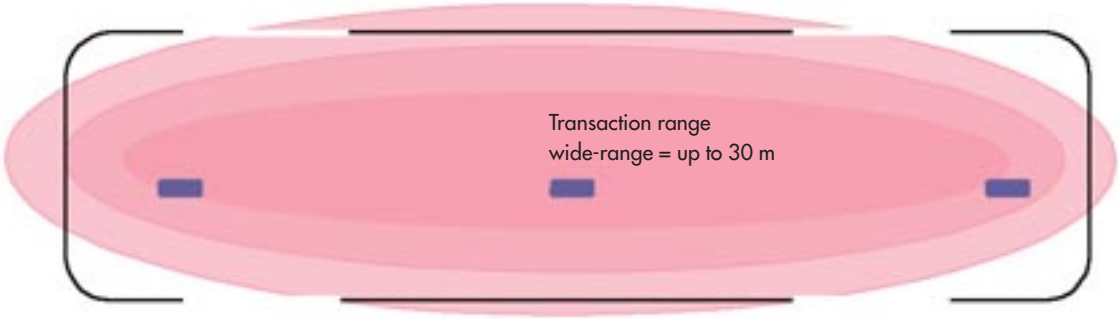
The customer carries a card with a wide-range transponder system. He/she can freely decide on his/her future route, in accordance with his/her departure and destination wishes.

Each time the vehicle approaches a new station, automatic detection of all chip cards present in the vehicle takes place (Bi). When the customer exits the vehicle, the card is no longer registered at the next detection; the passenger is considered to have exited (Bo).

The radio beam (866 MHz or 2.45 GHz) must be able to make unobstructed contact with the transponder. Hence, the customer must take care that the medium is not carried in a transmission-resistant container.

Location of 1 to 3 transmission/reception antennae inside the vehicle

FIG. 3.5.3



3.5.4 Combinations of these techniques

By combining the various techniques illustrated above, technical advantages can be used and potential problems inherent in a system, such as the customer's forgetting to check out, can be remedied. In this way, a secure and reliable registration of each trip and the corresponding trip data can be ensured.

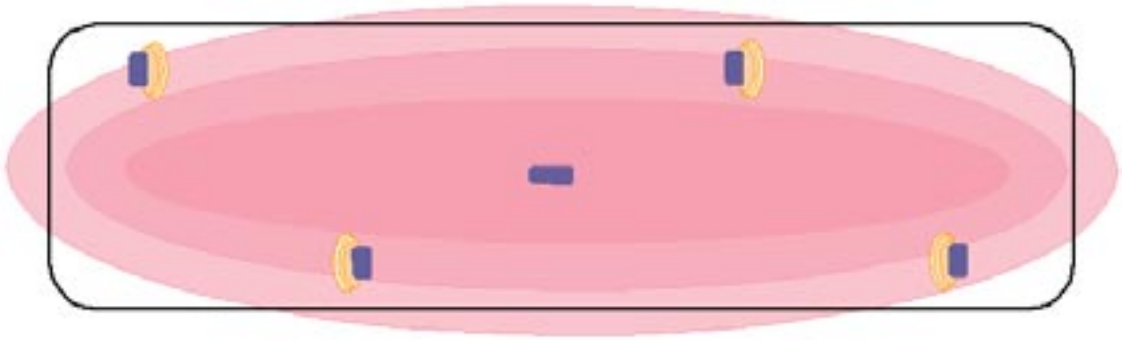
Two combinations lend themselves especially to this task; they necessitate either a single action on the part of the passenger or merely a passive carrying of the electronic ticket with the passenger.

3.5.4.1 Check-in, be-out (CiBo)

Upon boarding, an action on the part of the customer is necessary (active check-in). The subsequent automatic detection records only the chip cards registered by check-in.

Mixed arrangement of CiCo terminals and transmission/reception antennae

FIG. 3.5.4.1

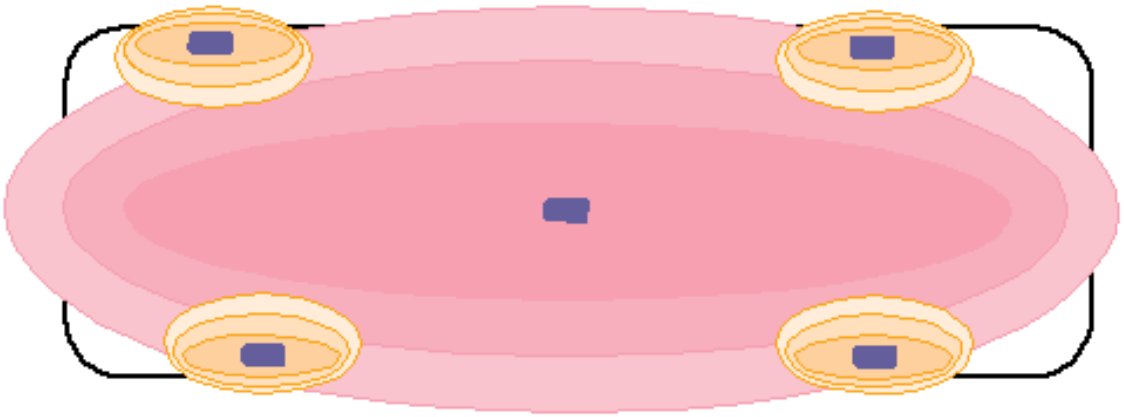


3.5.4.2 Walk-in, be-out (WiBo)

Upon boarding, the card is automatically activated in the entrance area (walk-in). The subsequent detection, also automatic, records the chip cards registered in this manner; exiting is again automatically detected (be out).

Mixed arrangement of walk-in antennae and transmission and reception antennae for detection

FIG. 3.5.4.2



3.6 Ticketing procedures

In addition to the familiar eTicketing procedures via chip cards, other possibilities with which an electronic ticket can be generated, paid, and used by the passenger have recently begun to be discussed and investigated.

eTicketing via mobile telephone, internet, and PDA will now be described briefly.

eTicketing via mobile telephone (mobile ticketing)

Prerequisites for mobile ticketing via mobile telephone:

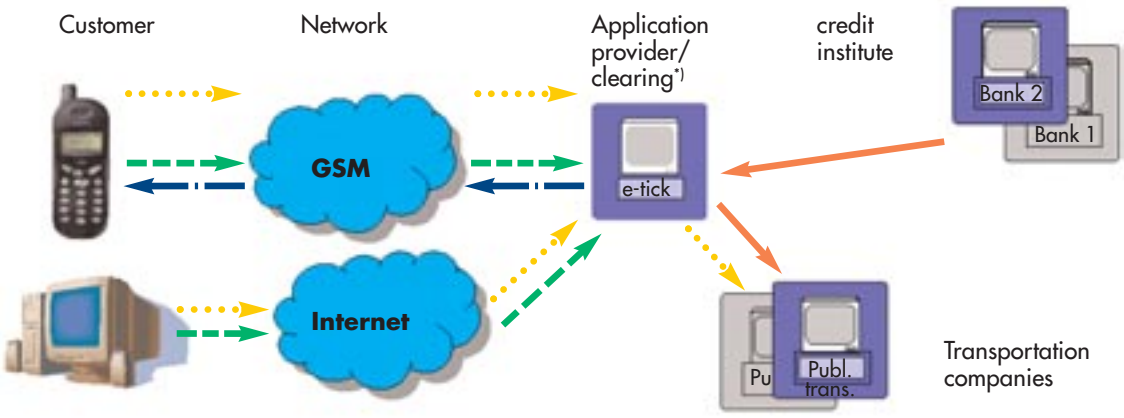
- Roaming standards for secure payment transactions
- Integration of all relevant mobile providers, credit institutes, and application providers in this procedure (booking from provider, bank, or credit card account possible)

Advantages of this procedure:

- High degree of availability and acceptance of the terminals (mobile telephones) and the network
- Simple, uncomplicated operation
- Low investment by the transportation company in the infrastructure
- Simple realization of national and even international mTicketing solutions possible
- Use of the new MMS (multimedia SMS) technology for counterfeit-proof depiction of eTickets on the mobile display
- Customer can be localized via the localization services of the mobile provider
- Implementation of additional services for the customer (e.g. up-to-date departure times, location of the next stop, best pricing, etc).

Acquiring an electronic ticket via mobile telephone or PC

FIG. 3.6.1



*) Application provider only necessary if several transportation companies are involved. Otherwise carried out by transportation company itself.

Customer registration (requested from application provider via PC or mobile telephone)

Ticket request (requested from application provider via PC or mobile telephone)

Ticket confirmation (signaled and stored in mobile telephone)

Money flow (booking according to previous consent by the customer (upon registration))

Disadvantages of this procedure:
- Standards and agreements governing mobile transactions (transaction roaming) still lacking; hence involvement of only regional providers possible
- Fallback solutions for customers without mobile telephones must continue to be provided for
- Depiction of several fares on the mobile display

Acquiring an electronic ticket via the internet

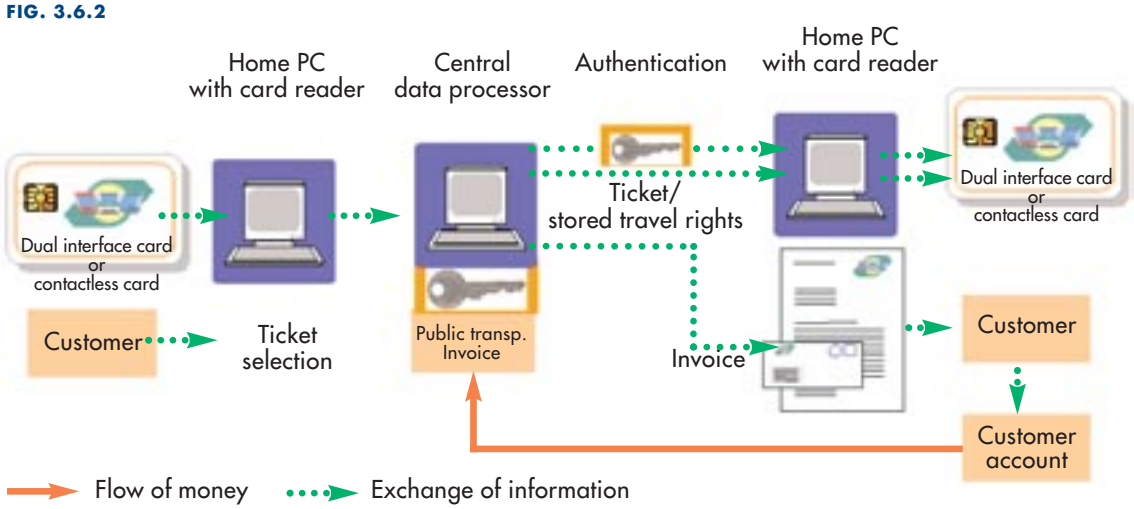
The prerequisites for mobile ticketing via internet: account at mobility provider, valid identification medium, password, card reader on the home PC.

The customer logs on to the system with the identification medium and password; after specifying the desired trip, the ticket is stored on his/her customer medium. It can then be used to travel on public transportation. The customer can also load travel rights into storage.

The advantages of this procedure:
Secure and uncomplicated, the necessary network already exists, strong market penetration.

Acquiring an electronic ticket via internet

FIG. 3.6.2



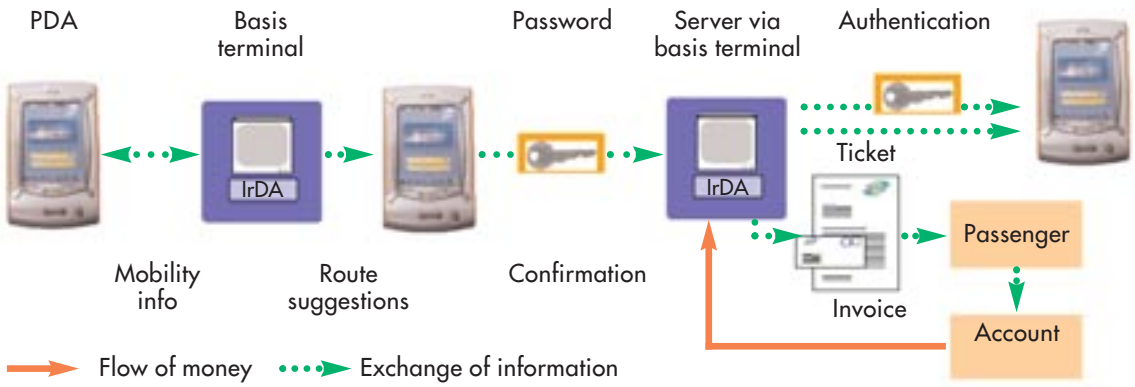
Acquiring a ticket via PDA (personal digital assistant)
The prerequisites for mobile ticketing via PDA:
special program for PDA/IrDA basis terminals that communicate with the mobility provider/account at the mobility provider / password

Advantages of this procedure:
Large display, rapid transmission of data, sensible data storage

Disadvantages of this procedure:
Own network required, basis terminal and special software necessary, currently little market penetration, only one connection at a time possible

Acquiring a ticket via PDA (personal digital assistant)

FIG. 3.6.3



3.7 End devices

3.7.1 Device types

With the introduction of a contactless fare management system, sales channels will be reorganized to be more open and transparent. In conjunction with innovative and well-engineered end devices, these new forms of tickets enable simplified access to public transportation.

Uniform operator guidance in surmounting obstacles increases the acceptance of the system amongst passengers. The attractiveness of public transportation is thus increased, and satisfactory results can be achieved.

Because of the complexity of the individual applications, a range of device types is necessary.

The following list describes the potential device types:

- issuing terminal
- loading terminal
- ticket window terminal
- info-terminal
- multi-terminal
- check-in/check-out terminal
- be-in/be-out terminal
- walk-in/walk-out terminal
- driver terminal
- control terminal
- "value checker," wallet, shell
- home terminal (internet)
- terminal for returning cards
- terminal for collecting cards
- mobile telephone
- PDA
- tags

Types of end devices and their range of application

FIG. 3.7.1

	Issue card	Payment function	Loading	Check-in/ Check-out	Walk-in/ Walk-out Be-In/be-Out	Print receipt/ ticket	Generation	Information	Public transportation initialization	Pre-selection	Ticket inspection	Card collection/ return
Issuing terminal		x	x			x	x	x	x	x		
Loading terminal	x	x	x			x[3]	x					
Ticket window terminal	x	x	x			x	x	x	x	x	x	
Multi-terminal	x	x	x	x	x	x	x	x	x	x	x	x
Check-in/ Check-out terminal		x[1]		x								
Driver terminal		x	x	x	x	x[3]		x	x	x	x	
Control terminal		x[2]				x					x	
"Value checker" wallet, shell								x		x		
Home terminal (internet)		x	x			x	x	x	x	x	x	
Terminal for returning cards						x[3]						x
Terminal for collecting cards												x
Mobile telephone		x	x	x	x		x	x		x		
PDA		x	x	x	x		x	x		x	x	
Tags		x	x	x	x							

[1] *Check-out payment* [2] *penalty fee* [3] *receipt*

A sensible selection must be made, depending on the application.

3.7.2 Functionalities

- In security-relevant transactions, use of SAM (security access module, type A&B) for handling all data (mobile/stationary)
- Combined reader for types A&B, as well as contact-type/contactless
- Writing of multiple data fields

3.7.3 Interfaces

The interfaces described in the following guarantee a smooth flow of data. The integration of the individual components is determined by the existing infrastructure.

3.7.3.1 Interfaces, vehicle

- CAN Bus
- IBIS
- RS 232
- RS 485
- ETHERNET

3.7.3.2 Interfaces, vehicle/depot

- GSM/GPRS/EDGE
- GPS/UMTS
- Wireless LAN

- Private mobile radio
- Trunked mobile radio
- Radio beacon
- Infrared
- Bluetooth

3.7.3.3 Interfaces, depot/headquarters

- GPS
- GSM/GPRS/EDGE
- UMTS
- LAN
- Analog/ISDN modem
- Bluetooth

3.7.4 Trends in development

- POS terminal: division of operating system and applications (e.g. OTA (open terminal architecture))
- GSM telephones: will become card terminals, on the basis of the GSM11.14 SIM toolkit
- PC: ➜ will become a platform-independent card terminal
  ➜ chip cards will be integrated (terminal-independent) in PC programs

3.8 Background system

The following description of the tasks and components of a background system for electronic ticketing outlines only the fundamental characteristics; complete detailed description is beyond the scope of these Recommendations for Action.

3.8.1 Tasks of the background system

Master data management

- Partners (points of sale, points of acceptance, individual customers,...)
- Cards (customer data)
- Terminals
- Fares, individual services, and sales packages (products)
- Calculation rules for purchase and selling prices

Transaction data management

- Maintaining the agency accounts for the cards
- Creation of services and sales catalogs
- Clearing of prepaid products (e.g. wallets)
- Determination of services provided in the case of postpaid products
- Calculation of prices based on calculation rules (cycle-oriented)
- Settlement with points of sale and points of acceptance
- Settling money flows with partners
- Price calculation of the individual services and packages

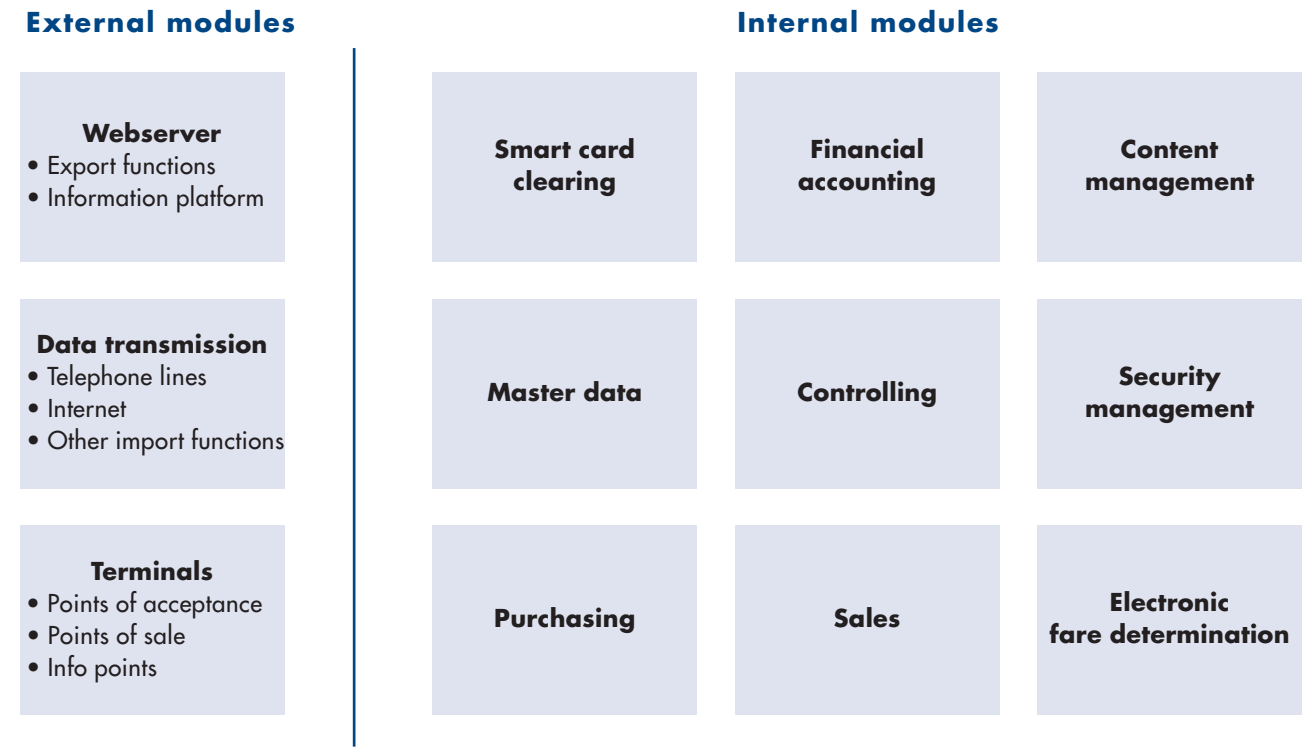
Cross-divisional functions

- Flexible reporting
- Individual design of correspondence (invoice layouts, etc)
- Import and export functions (Excel, XML, HTTPS, ...)
- Management of customer service (including the hotline interface)

3.8.2 Components in the background system

Components in the background system

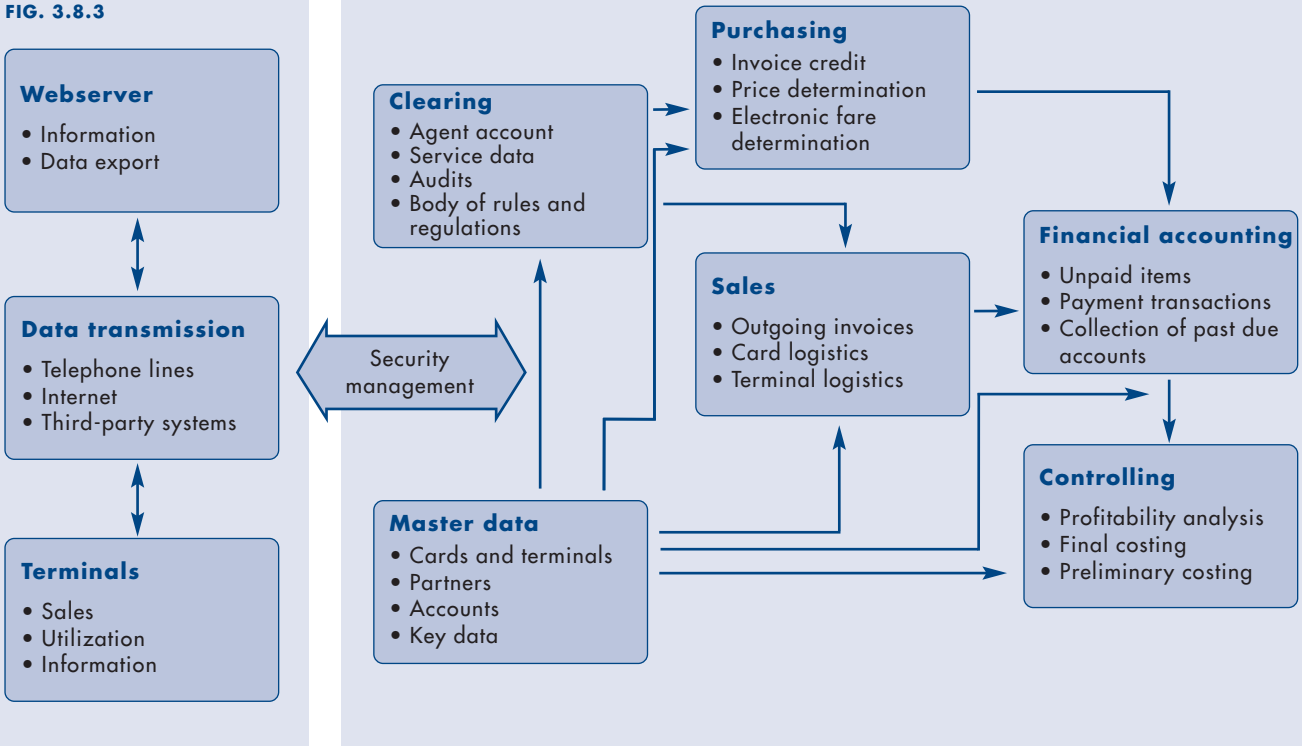
FIG. 3.8.2



3.8.3 Flow of data in the overall system

Flow of data in the overall system

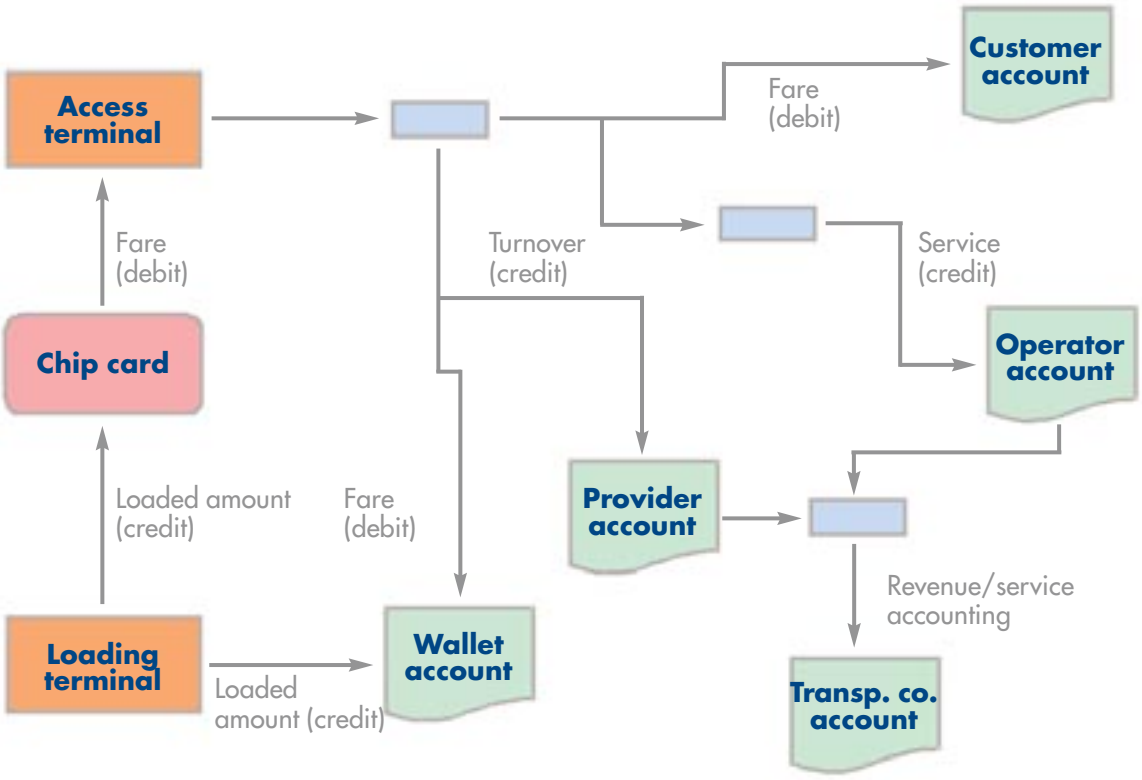
FIG. 3.8.3



3.8.4 Clearing and revenue accounting

Clearing and revenue accounting, here using the example of a chip card-based eWallet

FIG. 3.8.4



3.9 Interoperability and standardization

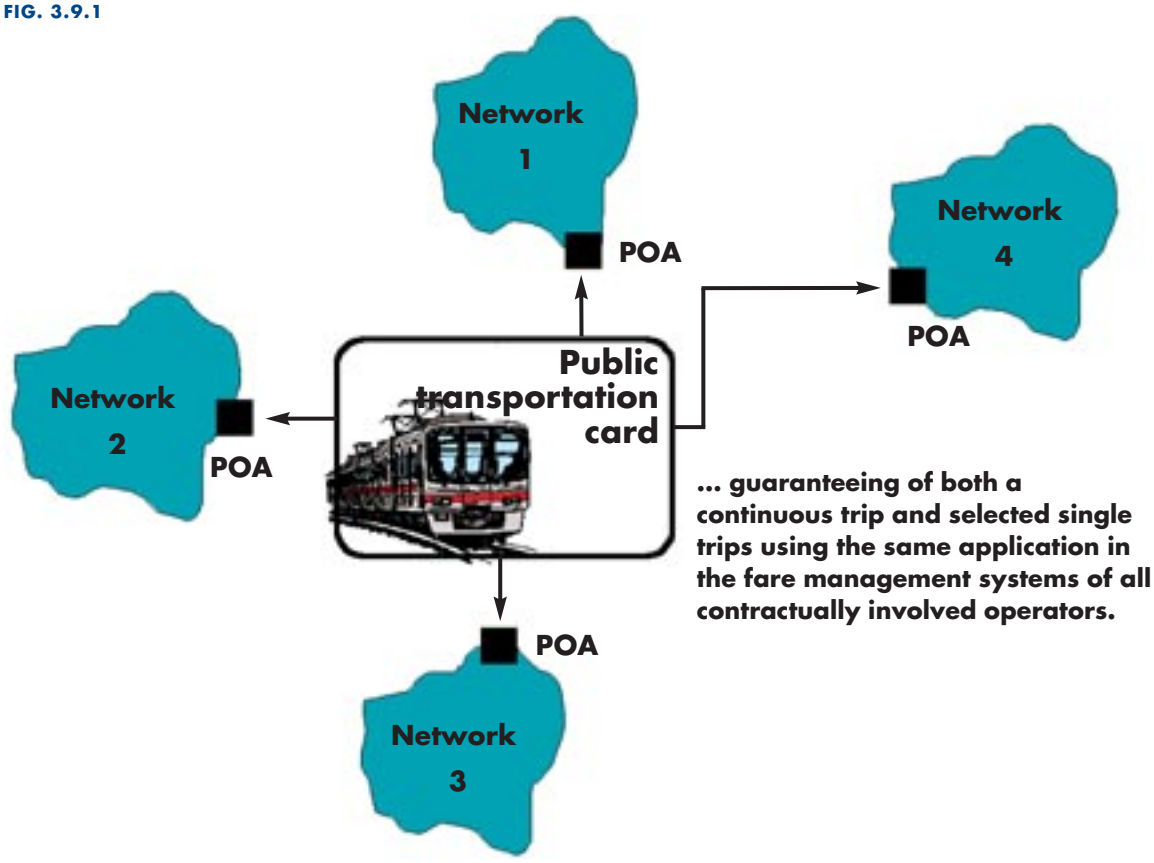
If the interoperability of a ticketing system is not to be based on bilateral agreements alone, but should instead be uniformly extendable up to and including international application, standardization of technical components and interfaces is indispensable.

This is already clear from the general definition of the term interoperability. "Interoperability is the ability of systems to provide services to and accept services from other systems and to use these services to enable the systems to operate effectively together" (Reference: CARDME Concerted Action on Research on Demand Management in Europe).

Specifically in public transportation, this means the following:

Interoperability in public transportation is ...

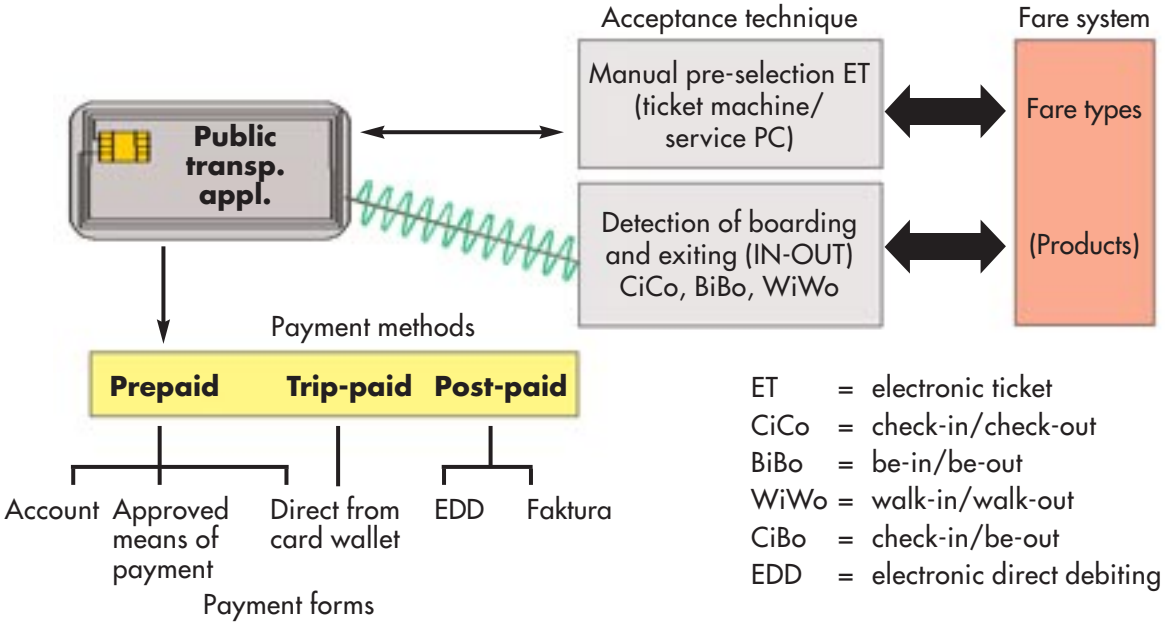
FIG. 3.9.1



Hence the interoperable application must support all acceptance techniques, fare systems, payment types and methods in the networks of all contractually involved operators.

Clearing and revenue accounting, here using the example of a chip card-based eWallet

FIG. 3.9.2



It becomes clear what degree of complexity the public transportation application must represent.

One feature of this representation is the decoupling of the carrier medium from the actual application. It should make no difference to the application on what carrier medium it runs. It must likewise make no difference to the carrier medium what applications run on it. The carrier medium must be able to host several applications (multi-application capability). In turn, each application is a vehicle for one or more functionalities.

This necessitates special organizational forms of stipulations for mutual access. The requirements on the standardization of the technical components are accordingly high.

However, "standardized" does not necessarily mean interoperable. Only when all development layers (ISO/OSI layers) of systems that want to communicate with each other comply with international standards can interoperability be assumed (see also comments in the German version of the Recommendations for Action 2000, p. 39).

In terms of standards for the purely technical development levels of smart cards, no new developments have taken place since 10/2000. The standards ISO/IEC7816 (contact-type cards, operating systems), ISO/IEC14443 (proximity ICs) and ISO/IEC15693 (vicinity ICs) are all available. Technical interoperability can thus be ensured; however, this does not mean that the applications as such behave in an interoperable manner.

In the past two years, great advances have been made in the standardization of the application-related development levels of smart cards specifically for public transportation. The revision of the standard for data elements for transportation applications (prEN1545) is already in the final formal European comment phase.

Application is defined as: data, commands, processes, states, mechanisms, algorithms, and program code within a chip, in order to operate it within the framework of a certain system.

This means that the documents

- identification card systems
- surface transport applications

Nomination documents

FIG. 3.9.3

Part 1: Elementary data types, general code lists, and general data elements

Part 2 : Transport's and travel's payment-related data elements and code lists

have been completed and will now be analyzed by experts in the respective countries, and corrected and supplemented as needed. At the end of this 6-month process (10/2003) and after integrating the comments, formal voting on the European Standard EN1545 will follow. This is expected at the end of 2003.

The elaboration of the interoperably interpretable data structures for public transportation applications (IOPTA, Interoperable Public Transportation Applications) is already in the working draft stage. An initial informal commenting phase at the European level is expected at the end of the third quarter of 2003.

Through the active participation of kontiki members, the interests of the VDV core application are being pursued in both EN1545 and IOPTA.

In the course of developing these smart card standards, the necessity of additional standardization work has become evident. If interoperability is to be achieved, the architecture of an electronic ticketing system, from the specification of participants active in the process and the general security architecture to the clearing processes between the participants, must be characterized by extensive standardization.

Standardization work in
- interoperable public transport
- fare management system architecture

is currently being carried out in CEN (TC278/WG3/SG5).

Initial results with respect to the logical roles in an EFM system have already proven themselves within the framework of work on the VDV core application, and have in turn been significantly influenced by it.

See Chapter 2.5 for more details.

Conclusion

The necessary standards for creating an interoperable public transportation application already exist, or at least their basic features are available. Developing an EFM system based on smart cards without taking these standards into consideration can no longer be advocated today. This statement must especially be taken into consideration in preparing calls for bids, drafting specifications, and selecting suppliers for EFM systems.