Teil 1

MKT-Basiskonzept

Version 0.9

28.07.95

GMD - Forschungszentrum Informationstechnik
Projektbüro Dr. Debold
Zentralinstitut für die Kassenärztliche Versorgung

Die Weitergabe des Dokuments an Dritte ist ausdrücklich erlaubt.
Änderungen und Ergänzungen sind den Autoren vorbehalten.
Gewährleistung und Haftung sind ausgeschlossen.

Inhalt

1. Zweck 3

2. Referenzen 3

3. Abkürzungen 3

4. Basis-Konzept 3

4.1 Das ´Card Interface Environment´ 3
4.2 Logische Komponenten des MKT-Steuerungsprogramms 4
4.3 MKT-Varianten 4
4.4 Ansteuerung mehrerer MKTs 5

5. Besondere Eigenschaften 5

5.1 Display und Tastatur 5
5.2 Spannungsversorgung 5
5.3 Chipkarten-Größen 6
5.4 Downloading 6

1. Zweck

Zweck dieser Spezifikation ist es, das Basis-Konzept für Multifunktionale Kartenterminals (MKT) darzustellen. Ein MKT kann als Einbauversion oder als externes Endgerät ausgeprägt und mit einer oder mehreren Schnittstellen für kontaktorientierte Speicher- und Prozessor-Chipkarten ausgestattet sein.

2. Referenzen

Deutsche Telekom, GMD, RWTÜV, TeleTrusT Deutschland: 1995
CT-API 1.1 - Anwendungsunabhängiges Card-Terminal Application Programming Interface

TeleTrusT Deutschland: 1995
CT-BCS - Anwendungsunabhängiger CardTerminal Basic Command Set

DIN 66003: 1974
Deutsche Referenzversion mit Umlauten

ISO/IEC 7810: DIS 1995
Identification cards - Physical characterisitics

ISO/IEC 7816-2: 1988
Identification cards - Integrated circuit(s) cards with contacts
Part 2 - Dimensions and location of contacts

ISO/IEC 7816-4: 1995
Identification cards - Integrated circuit(s) cards with contacts
Part 4 - Inter-industry commands for interchange

CEN ENV 1375-1: 1994
Identification card systems - Intersector integrated circuit(s) card additional formats - Part 1: ID-000 card size and physical characteristics

CEN prEN 1332-5: 1994 (Draft)
Identification card systems - Man-machine interface - Part 5: Key pads

3. Abkürzungen

API = Application Programming Interface
CIE = Card Interface Environment
CT = Card Terminal
HTSI = Host Terminal Software Interface
ICC = Integrated Circuit(s) Card
MKT = Multifunktionales Kartenterminal
SDA = Serial Data Access
2WB = 2 Wire Bus
3WB = 3 Wire Bus

4. Basis-Konzept

4.1 Das ´Card Interface Environment´

Das Anwendungssystem in einem PC oder in einer Workstation wird auf eine anwendungsunabhängige Schnittstelle für die Integration der Chipkartentechnik (Card Interface Environment) aufgesetzt. Verwendung findet hier die CT-API-Schnittstelle, die folgende Basisfunktionen bietet:

- eröffnen des Kommunikationskanals (CT_API-Funktion CT_init),
- übertragen eines Kommandos und Rücklieferung der Antwort (CT_API-Funktion CT_data), und
- schließen des Kommunikationskanals (CT_API-Funktion CT_close).

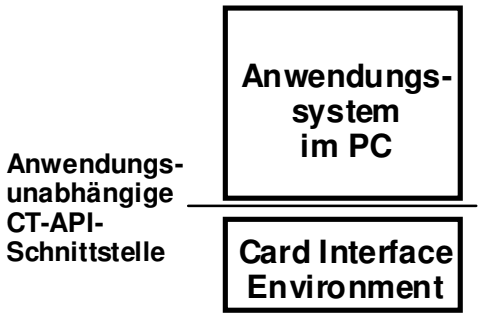


Abb. 1: Anwendungssystem mit Card Interface Environment

An der CT-API-Schnittstelle werden über die CT_data-Funktion die Chipkarten- und Kartenterminal-Kommandos übergeben. Als Kartenterminal-Kommandos ist der anwendungsunabhängige CardTerminal Basic Command Set zu verwenden.
Oberhalb der CT-API können höherwertige APIs (z.B. Security-APIs) Verwendung finden, die jedoch nicht Gegenstand dieser Spezifikation sind.

Das Card Interface Environment besteht aus

- einer Hardware-Komponente, dem MKT, und
- einer Software-Komponente, dem HTSI-Modul (Host-Terminal-Software-Interface Modul).

Zwischen HTSI-Modul und MKT liegt die MKT-Interface-Schnittstelle, deren Ausprägung MKT-abhängig ist.

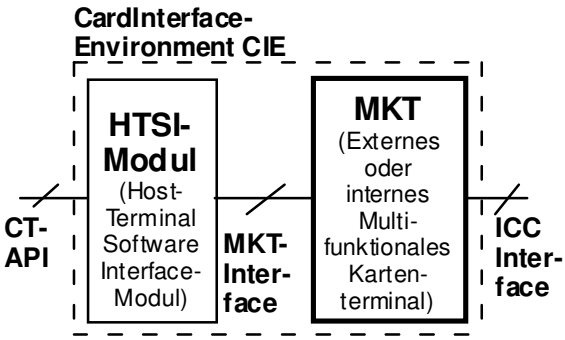
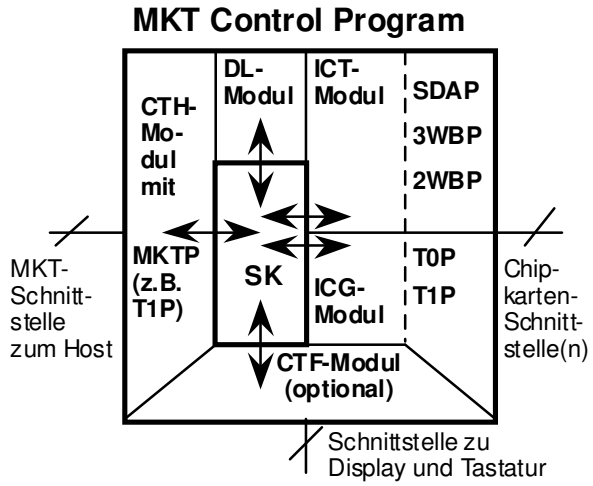


Abb. 2: Card Interface Environment

Das Card Interface Environment wird vom MKT-Hersteller bereitgestellt. Das Anwendungssystem kann daher vom Anwendungssystem-Hersteller mit verschiedenen MKTs ausgestattet werden, ohne daß an dem Anwendungssystem spezielle Anpassungen notwendig werden.

4.2 Logische Komponenten des MKT-Steuerungsprogramms

Ein MKT ist mit einem MKT Control Program ausgestattet, dessen logischen Aufbau Abb. 3 zeigt.



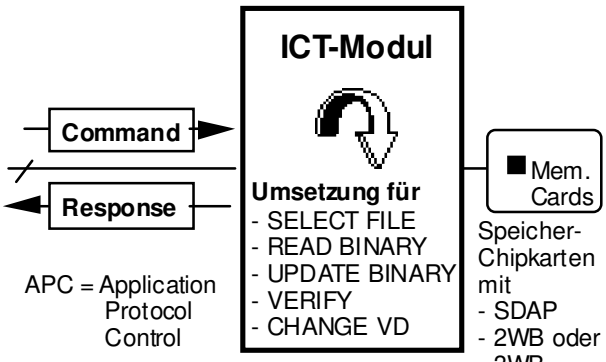
CTF = CT Function	MKTP = MKT Protocol
CTH = CT/Host	SDAP = SDA Protocol
DL = Download	SK = System Kernel
ICG = Inter-ind. Command Gateway	T0P = T=0-Protocol
	T1P = T=1-Protocol
ICT = Inter-ind. Command Transformation	2WBP = 2WB Protocol
	3WBP = 3WB Protocol

Abb. 3: Logischer Aufbau des MKT Control Program

Der ICT-Modul im MKT ist so konstruiert, daß an der CT-API-Schnittstelle ISO/IEC 7816 Inter-industry Commands für die Kommunikation mit Speicher-Chipkarten verwendet werden können. Dies

- erleichtert die Koexistenz von Speicher- und Prozessor-Chipkarten und
- erlaubt die einheitliche Ansteuerung unterschiedlicher Speicher-Chipkarten aus der Sicht des Anwendungssystems.

Nach Bedarf sollen in das MKT auch Anwendungsprotokoll-Kontroll-Module (z.B. zur Überwachung der Kommunikation mit der Versichertenkarte) integriert werden können.



Anmerkungen:
1. Die Kommandos SELECT FILE, READ BINARY und UPDATE BINARY sind die Inter-industry Commands für Grundfunktionen (in MKTs für Arztpraxen sind für die KVK-Anwendung nur die Kommandos SELECT FILE und READ BINARY zulässig).
2. Die Kommandos VERIFY und CHANGE VD sind die Inter-industry Commands für Sicherheitsfunktionen und nur anwendbar auf Chipkarten mit Sicherheitscode

Abb. 4: ICT-Modul

4.3 MKT-Varianten

Das MKT kann als

- integrierte Systemkomponente (z.B. Kartenleser integriert in die Tastatur, Kartenleser in einem Diskettenschacht, Kartenleser in einem PCMCIA-Modul) oder
- als separates Endgerät

ausgeprägt sein. Das MKT in der Ausprägung als separates Endgerät kann mit folgenden Zusatzoptionen ausgestattet sein:

- Display und Tastatur,
- zweite Kontaktiereinheit für eine Chipkarte im Normalformat gemäß ISO/IEC 7816-2 oder
- zweite Kontaktiereinheit für eine Chipkarte im Plug-in-Format.

Daraus ergibt sich das Konzept einer MKT-Familie, wie nachfolgende Tabelle zeigt (es sei darauf hingewiesen, daß auch weitere Kombinationen von Funktionseinheiten und mehr als zwei ICC-Schnittstellen möglich sind).

MKT-Familie				
Funktion / Bezeichnung	Grundfunktionen und eine Kontaktiereinheit	Display *und* Tastatur	2. Kontaktiereinheit für Normal-Chipkarte	2. Kontaktiereinheit für Plug-in-Chipkarte
MKT - I	+			
MKT - IN	+		+	
MKT - E	+			
MKT - D	+	+		
MKT - DN	+	+	+	
MKT - DP	+	+		+
MKT - N	+		+	
MKT - P	+			+

I = Internal Basis Version
E = External Basis Version
D = Version mit Display/Tastatur
N = Version mit 2. Karte in Normalgröße
P = Version mit Plug-in-Karte

Tab. 1: MKT-Familie

MKTs mit anderen Zusatzoptionen wie z.B. Sicherheits-Modul oder biometrische Identifizierungseinheit sind nicht Gegenstand dieser Spezifikation.

4.4 Ansteuerung mehrerer MKTs

Da bestimmte Anwendungen mit mehr als einer Chipkarte arbeiten (z.B. Arztkarte und Patientenkarte), kann der Anschluß von zwei MKTs notwendig sein. Falls hierbei MKTs eingesetzt werden, die unterschiedliche HTSI-Module bzw. CT-API-Libraries (siehe CT-API-Spezifikation) erfordern, so ist die Ansteuerung der unterschiedlichen HTSI-Module über die Benutzung von ´well known identifers´ (Hersteller-Kennung mit HTSI-Identifier) in den CT-API-Funktionsnamen möglich.

5. Besondere Eigenschaften

5.1 Display und Tastatur

Die Größe des Display - falls vorhanden - sollte mindestens die Darstellung von 2 Zeilen mit 16 Zeichen zulassen. Als Zeichenvorrat sind die Groß- und Kleinbuchstaben inklusive Umlaute sowie die üblichen Sonderzeichen zu unterstützen (Codierung entsprechend DIN 66003).
Falls eine Eingabetastatur vorhanden ist, sind folgende Regelungen zu beachten:

Falls eine 12er-Tastatur verwendet wird, ist die 11. und 12. Taste als

- Abbruchtaste und
- Bestätigungstaste

vorzusehen.

Falls eine 16er-Tastatur verwendet wird, sind neben den Zifferntasten

- Abbruchtaste
- Korrekturtaste und
- Bestätigungstaste

vorzusehen. Auf eine ergonomisch günstige Ausprägung ist zu achten. Bezüglich der Anordnung der Tasten sei auf die Norm CEN prEN 1332-5 hingewiesen.

5.2 Spannungsversorgung

Bei Kartenterminals, die mit mehreren Chipkarten-Schnittstellen arbeiten, ist die Spannungsversorgung so auszulegen, daß alle Chipkarten gleichzeitig mit Strom versorgt werden können. Genauere Angaben zur Stromaufnahme von Chipkarten sind in dem Dokument ´CT-ICC-Interface´ zu finden.

5.3 Chipkarten-Größen

Kartenterminal mit einer ICC-Schnittstelle sollen die übliche Kartengröße (ID-1, siehe ISO/IEC 7816-2) unterstützen. Ist eine zweite ICC-Schnittstelle vorhanden, so kann diese entweder als

- ID-1-Schnittstelle oder als
- ID-000-Schnittstelle (Schnittstelle für eine ´Plug-in-Karte´)

ausgeprägt sein. Abb. 5 zeigt die Relation von Chipkarten der Größe ID-1 (definiert in ISO/IEC 7810) und ID-000 (definiert in ENV 1375-1).

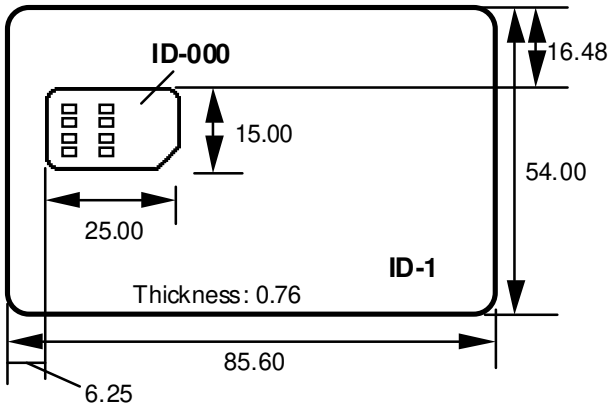


Abb. 5: Relation der Chipkarten ID-1 und ID-000

5.4 Downloading

Um Leistungsanpassungen vornehmen, Anzeigetexte für das Display (falls vorhanden) laden oder Fehler beheben zu können, müssen MKTs mit einer Download-Funktion ausgestattet sein. Der Download-Vorgang ist mindestens so abzusichern, daß kein Unbefugter die MKT-Software verändern kann (siehe Anhang CT-BCS-Spezifikation). Eine Realisierungsform ist, das Downloading mit einem separaten Ladeprogramm durchzuführen, das per Diskette für die verschiedenen Systemumgebungen bereitgestellt wird. Die Integrität und Vollständigkeit der Lademodule muß durch den Download-Modul im MKT prüfbar sein.