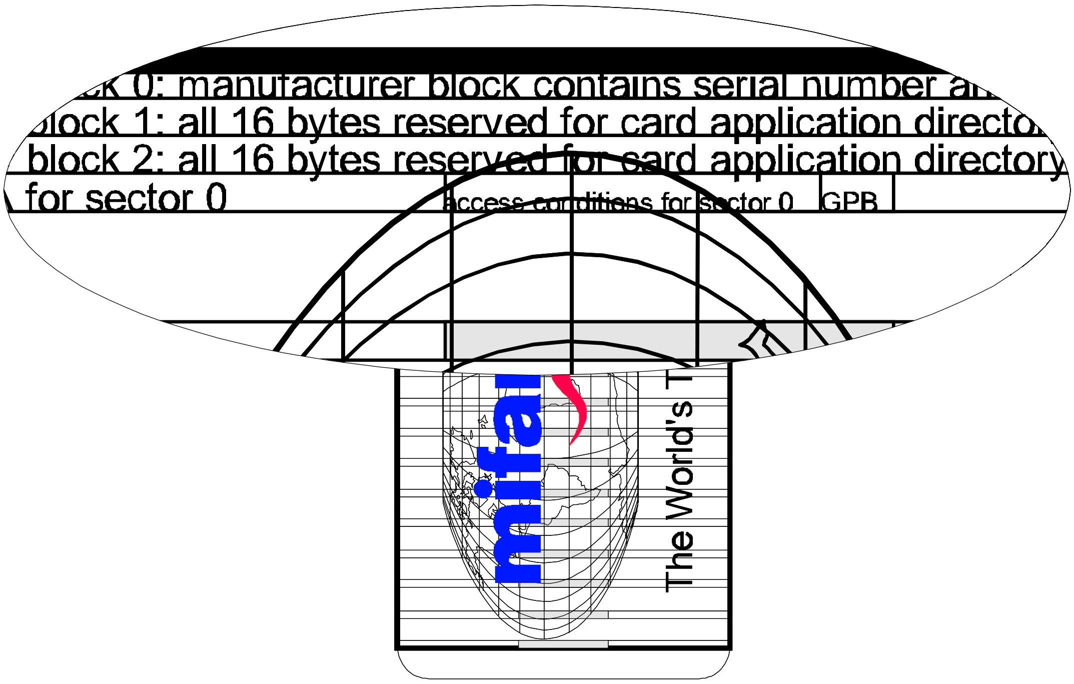
mifare®
standardization group

STANDARDIZATION NOTE

MIFARE® Application Directory MAD

date: 31.07.1998 / page 1 of 11 / Rev.: 1.1/ Auth.: RM



...k 0: manufacturer block contains serial number a...
...lock 1: all 16 bytes reserved for card application directo...
block 2: all 16 bytes reserved for card application directory
... for sector 0
access conditions for sector 0
GPB
mifa...
The World's T...

observing the following proposed

mifare® application directory rules

opens a lot of future benefits:

basic requirements	⇒ additional information	⇒ additional flexibility
• reserve 2 blocks • keep to given format • request for AID[1] • use public *read-key* for sector 0 • use secret *write-key* for sector 0 • use indirect addressing mode in terminal program	⇒ identify any application on any mifare® card together with the sectors in use ⇒ identify card issuer ⇒ identify free or blocked sector	⇒ already existing mifare® cards may serve for new additional applications ⇒ already existing mifare® applications on multiple cards may be combined on one single card ⇒ easy adaptation of memory structure in case of additional features or blocked sectors

[1] AID application identifier request formular can be found in annex A

SCOPE

The mifare® application directory standard proposes the introduction of common data structures for card application directory entries. Registered application identifiers (AID´s) in block 1 and 2 of any mifare® card enable identification of all registered card applications. Terminal software should take advantage of this feature using those sector pointers instead of physical sector addresses.

In the future it might easily happen that there are more than one mifare® card in a person´s wallet. The comfort of not having to take out the card of one´s wallet should be possible also with more mifare® cards in one wallet. A typical case can be that one person has cards for different applications (e.g. airline miles collection and city fare collection). With the MAD the airline check-in terminal identifies two cards and is able to choose the correct one very fast, simply by checking the MAD.

DATA ELEMENTS FOR APPLICATION DIRECTORIES AND SELECTION

Application identifier:

Is a unique 16 bit code divided into two fields:

<table>
<tr><td>bit
15</td><td></td><td></td><td></td><td></td><td></td><td></td><td>bit
8</td><td>bit
7</td><td></td><td></td><td></td><td></td><td></td><td></td><td>bit
0</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="8">(8 bit) function cluster code</td><td colspan="8">(8 bit) application code</td></tr>
</table>

To enable easy classification of the whole range of possible applications the function cluster code is used. Some codes are already prepared and outlined in annex C.

CRC-byte:

bit 7							bit 0

8 bits include a cyclic redundancy code according to the 8 bit CRC coprocessor. The coprocessor should be reset and afterwards the Info-byte and ID1 to ID$F (lower byte followed by higher byte) should be passed to the CRC coprocessor **exactly in this order**. This code allows an integrity check of the directory blocks.

Info-byte:

bit 7							bit 0
free				pointer to CPS			

4 bits include a binary number (01 to 0Fhex) pointing to one of 15 sectors belonging to the card publisher (card publisher sector CPS). 00hex should be used if the card publishing organization does not use any sector on the mifare® card. This information is particularly useful if somebody needs to find out the organization responsible for distribution of free card sectors for new applications. These free card sectors may easily be used for additional applications.

General purpose byte: (GPB)

The general purpose byte of the access condition field of sector trailer 0 describes further details of the MAD standard. It is the 10th byte of block 3. The code 69 hex should not be used for standardized cards and refers to non-personalized cards.

bit 7	bit 6					bit 1	bit 0
DA	MA	r.f.u.				ADV	

ADV	(MAD version code)	01	current MAD version 1
MA	(multiapplication card)	1	yes
		0	monoapplication card
DA	(MAD available)	1	yes
		0	*sector 0 does not contain MAD (all further MAD conventions are not considered)*

Read-key A:

Key A of sector 0 should be public and set to the following hex code:

byte 5					byte 0
a5	a4	a3	a2	a1	a0

Under specific circumstances key A may be changed and forwarded just to a limited number of organizations.

Write-key B:

Key B of sector 0 is programmed by the card issuer and should be kept secret. If additional applications join the same mifare® card key B may be forwarded to the organization which provides the new services in order to enable directory (MAD) adaptation during reinitialization of the mifare® cards.

CODING OF THE APPLICATION DIRECTORIES

MAD version numbers

This standard proposes MAD version 1. For future mifare® cards this MAD standard may change together with the version numbering. The version number is encoded in the GPB.

MAD types

This standard allows 3 types of MAD:

A	monoapplication card without directory entries	(code 00hex)
B	monoapplication card with directory entries	(code 10hex)
C	multiapplication card with directory entries	(code 11hex)

The MAD type is encoded in the GPB.

Function clusters

Function cluster codes enable easy classification of applications. Currently used codes may be found in annex C. Any organization requesting for a new AID may suggest a code out of this list. If this information is missing the registration authority will determine the code.

Administration codes

Function cluster code 00 hex assigns specific administration codes to the corresponding sector:

AID - administration codes	
00 00 hex	sector is free
00 01 hex	sector is defect, e.g. access keys are destroyed or unknown
00 02 hex	sector is reserved
00 03 hex	sector contains additional directory info (useful only for future cards)
00 04 hex	sector contains card holder information in ASCII format.

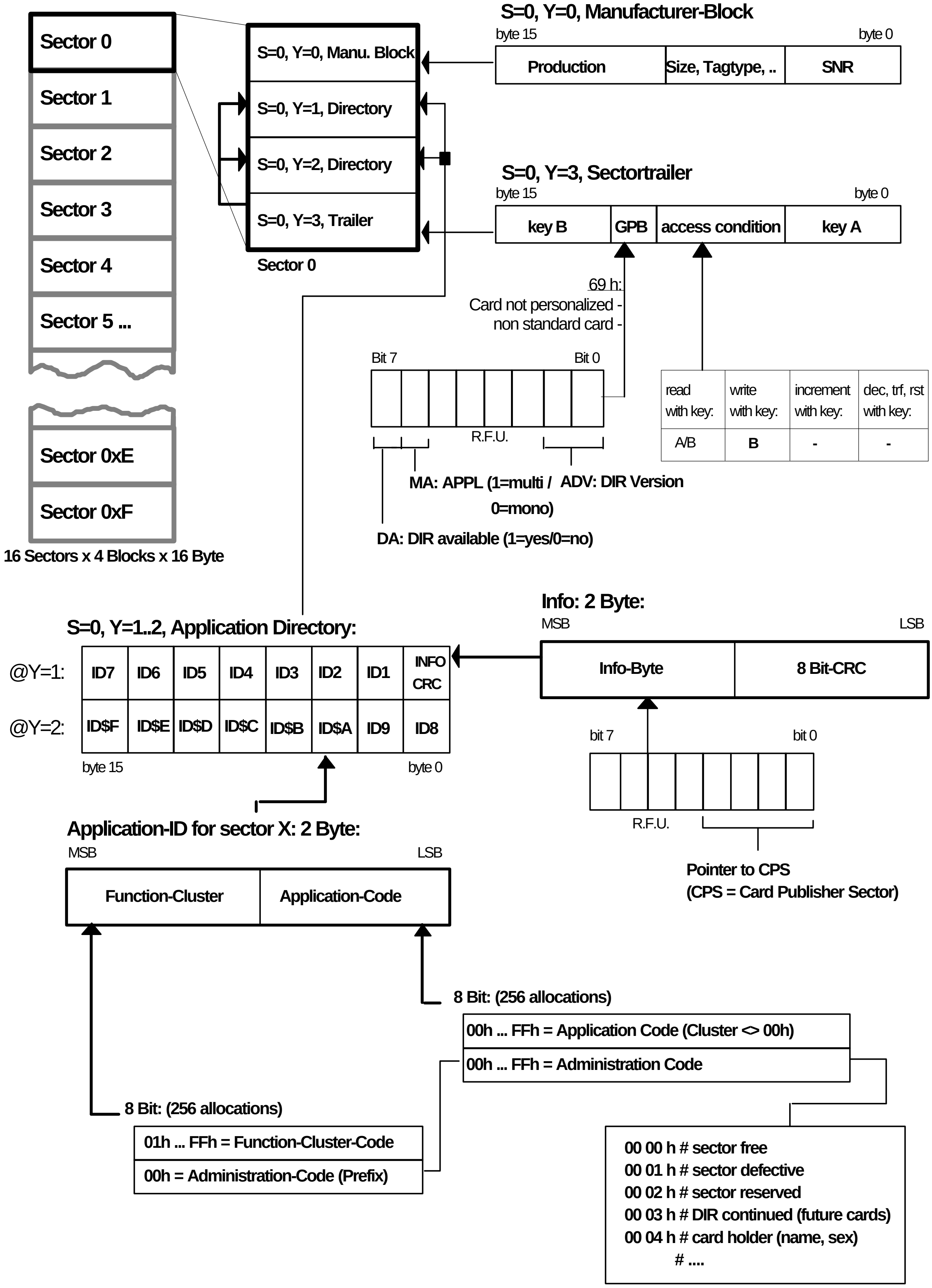
Card holder information

The administration code 0004 hex indicates to public *card holder information* in the corresponding sector. There is no binding rule but just the following recommendation given for storing card holder information using RLC (Run-Length-Coding):

				bit 7 bit 0
byte n	byte n-1		byte 1	byte 0
00	last character	...	character 1	**type length<n>**

byte 0: **length** = lower 6 bit (number of used bytes including 00 hex, max. 63)
type = highest 2 bit (**00**=*surname*; **01**=*given name*; **10**=*sex*; **11**=*any other data*)

continued at page 6



read with key:	write with key:	increment with key:	dec, trf, rst with key:
A/B	**B**	-	-

S=0, Y=1..2, Application Directory:

@Y=1:	ID7	ID6	ID5	ID4	ID3	ID2	ID1	INFO CRC
@Y=2:	ID$F	ID$E	ID$D	ID$C	ID$B	ID$A	ID9	ID8

00h ... FFh = Application Code (Cluster <> 00h)
00h ... FFh = Administration Code

01h ... FFh = Function-Cluster-Code
00h = Administration-Code (Prefix)

00 00 h # sector free
00 01 h # sector defective
00 02 h # sector reserved
00 03 h # DIR continued (future cards)
00 04 h # card holder (name, sex)
....

continued from page 4

byte 1 to <n>: ASCII text as specified in **type** (first character at byte 1; ends with 00 hex)

Unused bytes should be set to 00 hex. For storing the sex the following convention is suggested - use „m“ (code 6D hex) for masculin and „f“ (code 66 hex) for feminin. In case of insufficient storage space in one sector the card holder information may be continued in the next sector referenced by the administration code 0004 hex.

e.g: surname: Sampleman
given name: Philip
masculin
Tel+1/1234/5678
all data is readable with key A but key B is necessary for writing

the hexadecimal contents of the corresponding sector should look like this:

byte 15							byte 8	byte 7							byte 0
6C	69	68	50	**47**	00	6E	61	6D	65	6C	70	6D	61	53	**0a**
33	32	31	2F	31	2B	6C	65	54	**D0**	00	6D	**82**	00	70	69
00	00	00	00	00	00	00	00	00	00	38	37	36	35	2F	34
s	e	c	r	e	t	69	88	77	78	a5	a4	a3	a2	a1	a0

The card issuer is responsible for appropriate key protection of card administration sectors. It is advisable to protect all sectors of the card against unauthorized writing with secret keys B. This is recommended even for free and unused sectors.
In special cases, for example when storing *public card holder information* this data may be released for public reading using the default key A: a0a1a2a3a4a5 hex.

The location of each AID points to a specific sector on the card.

The location of an AID within sector 0 specifies the sector in use for the corresponding application.

schematic of sector 0:

	byte 14		byte 12		byte 10		byte 8		byte 6		byte 4		byte 2		byte 0
m	a	n	u	f	a	c	t	u	r	e	r	c	o	d	e
AID sector	for 7	AID sector	for 6	AID sector	for 5	AID sector	for 4	AID sector	for 3	AID sector	for 2	AID sector	for 1	info	CRC
AID sector	for 15	AID sector	for 14	AID sector	for 13	AID sector	for 12	AID sector	for	AID sector	for 10	AID sector	for 9	AID sector	for 8
s	e	c	t	o	r		t	r	a	i	l	e	r		0

CRC calculation

Byte 0 of block 1 will contain 8 bit cyclic redundancy code (CRC). It is generated at the generation of the MAD.

This code should be checked whenever the MAD is read in order to ensure data integrity. Both for the CRC generation and the CRC check the internal CRC coprocessor of the mifare® reader ASIC may be used. Actually the *mif_calc_crc()* function from the mifare® LowLevelLibrary allows an easy calculation of the CRC code.
The *Info* byte should be processed first, then ID1, ID2, ID3, ID4, ID5, ID6, ID7, ID8, ID9, ID$A, ID$B, ID$C, ID$D, ID$E, ID$F in this order. Always process the *lower byte first* within the AID´s followed by the higher byte. That means the following process order: block 1, byte 1 to byte 15, block 2, byte 0 to byte 15. Of course the calculation can also be achieved via appropriate software.
8 bit CRC uses the polynom: $\mathbf{x^8 + x^4 + x^3 + x^2 + 1}$ and is preset with **E3** hex

example for CRC calculation with a sample MAD (hex values):

	byte 14		byte 12		byte 10		byte 8		byte 6		byte 4		byte 2		byte 0
AID sector	for 7	AID sector	for 6	AID sector	for 5	AID sector	for 4	AID sector	for 3	AID sector	for 2	AID sector	for 1	info	CRC
00	04	00	00	00	00	00	00	08	01	08	01	08	01	01	89
AID sector	for 15	AID sector	for 14	AID sector	for 13	AID sector	for 12	AID sector	for 11	AID sector	for 10	AID sector	for 9	AID sector	for 8
30	11	00	00	00	00	00	00	10	02	10	02	10	03	10	03

Pointer to card publisher sector

The lowest 4 bits of the Info-byte contain a binary pointer to one of the 15 sectors in use. The owner of the corresponding sector is considered to be the card publisher, responsible for card issue, card maintenance and also for maintenance of the MAD. 00hex should be used if the card publishing organization does not use any sector on the mifare® card.

Key protection of MAD

Block 3 of sector 0 (sector trailer 0) contains key information as well as access condition information. The MAD should be well write-protected with a secret key B defined by the card issuer. Anybody should be allowed to read the MAD. This is achieved by using a public read key A:

key A: `a0a1a2a3a4a5 hex`

Access conditions should allow reading with key A|B and writing with key B. According to the mifare® card product specification this means the following code:

```
C1X0 C2X0 C3X0:  x  x  x  (don´t care for manuf.code)
C1X1 C2X1 C3X1:  1  0  0
C1X2 C2X2 C3X2:  1  0  0
C1X3 C2X3 C3X3:  0  1  1
```

example for sector trailer 0 with hex codes:

Type of example card: multiapplication with directory

byte15							byte 8	byte 7							byte 0
s	e	c	r	e	t	C1	88	77	78	a5	a4	a3	a2	a1	a0
key B						access condition				key A					

All currently unused sectors should be well write protected with secret write keys defined by the card issuer in order to prevent unintended redefinition of access conditions and keys. It is recommended to use different keys for all free sectors. This enables future release of some sectors to new service providers without the need of releasing all free sectors.

USE OF THE APPLICATION DIRECTORIES

Directory scan procedure

The purpose of the MAD is to gain additional information and flexibility. These benefits ask for specific proceedings of application software:
Any transaction should start with a directory scan; that means authentication of sector 0 with key A and reading at least blocks 1 and 2. In most cases block 3 is necessary to get general information about the directory structure found in the GPB of block 3.
The next step is to look for the relevant AID´s in the directory blocks which point to the actual sector addresses in use. Several identical AID´s may point to different sectors belonging to the same application. The data structure within the application sectors must be organized with application software. If sectors are changed during life time of the card application, the software needs specific algorithms for locating single data records in several sectors.

Indirect addressing mode

Data identification and manipulation algorithms should only use the indirect addressing mode by using the sector pointers which are extracted out of the MAD.

REGISTRATION OF APPLICATION IDENTIFIERS

Each mifare® application should be encoded in an unique AID. To achieve this goal a central registration authority is set up. Any organization may request for AID´s for new mifare® application free of charge using the attached registration form (see ANNEX A). The contents of sector B of this formular will be inserted in a common database.

mifare® STANDARDIZATION GROUP AND REGISTRATION AUTHORITY

The mifare® standardization group (MSG) is made up of several major organizations using the mifare® contactless smart-card in multiple applications.
The MSG has nominated PHILIPS Semiconductors, Austria, to deal with the issues of the registration authority. In addition it serves as contact address for any further requests:

PHILIPS Semiconductors GmbH
Mikron-Weg 1
A-8101 Gratkorn, Austria
MIFAREâ MAD Registration Office

Tel.: +43 / 3124 / 299 - 0
Fax : +43 / 3124 / 299 - 330
Email: info@grk.sc.philips.com

ANNEX A, Registration form[2]
REQUEST FOR REGISTERED APPLICATION IDENTIFIER (AID)

information in sector A is not published.

A. To be completed by the requesting organization

100 Name of organization		
101 Address for correspondence		
102 Principal contact in organization		
103 Telephone number	104 Fax number	105 Email address
106 Date	107 Signature	

information in sectors B and C will be published. The requesting organization may omit completition for parts of sector B if this should remain secret.

B. Data to be registered and published

201 Names of service provider organizations		
202 Names of technical system integration organizations		
203 Name of clearing house		
204 Description of application		
205 Suggested functional cluster		
206 Locations of application		
207 Number of sectors in use	208 Launching date	209 Number of desired AID´s
210 Please reserve the following AID´s	211 Please release the following reserved AID´s	

C. To be completed by the registration authority

310 AID granted	311 Functional cluster	
320 AID granted	321 Functional cluster	
330 AID granted	331 Functional cluster	
340 AID granted	341 Functional cluster	
390 Request received by	391 Date	392 Signature

[2] find help information on next page

ANNEX B, Help information for registration form

information in sector A is not published.

A. To be complet… ganization

100 Name of organization		
101 Address for correspo		
102 Principal contact in organization		
103 Telephone number	104 Fax number	105 E-mail address
106 Date	107 Signature	

the requesting organization will be responsible for correct administration and programming of AID´s

granted AID´s will be sent to this number

information in sectors B and C will be published. The requesting organization may omit completition for parts of sector B if this should remain secret.

B. Data to

201 Names of s		
202 Names of technical system integration organizations		
203 Name of clearing house		
204 Description of ap		
205 Suggested function		
206 Locations of applica		
207 Number of sectors in use	208 Launching date	209 Number of des
210 Please re… s	211 Please release the following reserved	

responsible for hardware and software integration and maintenance

if any ?
calculating balance between various service providers

describe all services available with the mifare® card

if any ?
the 8 most significant bits of the 16 bit AID refer to a functional cluster - outlined on next page

fill in name of towns, regions etc.

normally one AID per application will be sufficient, however in some cases serveral AID´s may be reserved

refers to start date of application

C. To be completed by the registration authority

310 AID granted	311 Functio
320 AID granted	321 Functio
330 AID granted	331 Functio
340 AID granted	341 Functional cluster
390 Re	

if any ?
if you know about specific reserved numbers or you suggest certain code numbers

if any ?
if you have reserved AID´s which are no more used release them as soon as possible, in case of future use please delay request for new codes until actually needed

will be granted by registration authority and sent via fax

will be granted by registration authority and sent via fax

ANNEX C, Functional cluster codes

(16 bit) AID code

bit 15							bit 8	bit 7							bit 0
(8 bit) function cluster code								(8 bit) application code							

function cluster codes

cluster code (hex)	**function**
00	card administration
01-07	miscellaneous applications
08	airlines
09-0F	*r.f.u.*
10	railway services
11-17	*r.f.u.*
18	city traffic
19-1F	*r.f.u.*
20	bus services
21-27	*r.f.u.*
28	taxi
29-2F	*r.f.u.*
30	road toll
31-37	*r.f.u.*
38	company services
39-3F	*r.f.u.*
40	city card services
41-47	*r.f.u.*
48	access control & security
49	VIGIK
4A-4F	*r.f.u.*
50	ski ticketing
51-57	*r.f.u.*
58	academic services
59-5F	*r.f.u.*
60	food
61-67	*r.f.u.*
68	non food trade
69-6F	*r.f.u.*
70	hotel
71-77	*r.f.u.*
78	car rental
79-7F	*r.f.u.*
80	administration services
81-87	*r.f.u.*
88	electronic purse
89-8F	*r.f.u.*
90	television
91-97	*r.f.u.*
98	telephone
99-9F	*r.f.u.*
A0	health services
A1-A7	*r.f.u.*
A8	warehouse
A9-AF	*r.f.u.*
B0	electronic trade
B1-B7	*r.f.u.*
B8	banking
B9-BF	*r.f.u.*
C0	entertainment & sports
C1-C7	*r.f.u.*
C8	car parking
C9-CF	*r.f.u.*
D0	fuel, gasoline
D1-D7	*r.f.u.*
D8	info services
D9-DF	*r.f.u.*
E0	press
E1-E7	*r.f.u.*
E8	computer
E9-EF	*r.f.u.*
F0	mail
F1-F7	*r.f.u.*
F8-FF	miscellaneous applications

r.f.u. reserved for future use