A Rambling Talk about an EMV Transaction.

Tim Becker

29c3

2012-20-12

About me.


YOURBANK
CREDIT CARD
1234 5678 1234 5678
Tim Becker
VALID FROM
EXPIRES END
08/07-08/10

Motivation.

No Hacks

Nothing new

Really old, actually.

Basics, Specs, TLAs

(Crypto)

Originally Windows

Supported on most OS

Bindings for most languages

https://github.com/costan/smartcard

https://github.com/a2800276/29c3

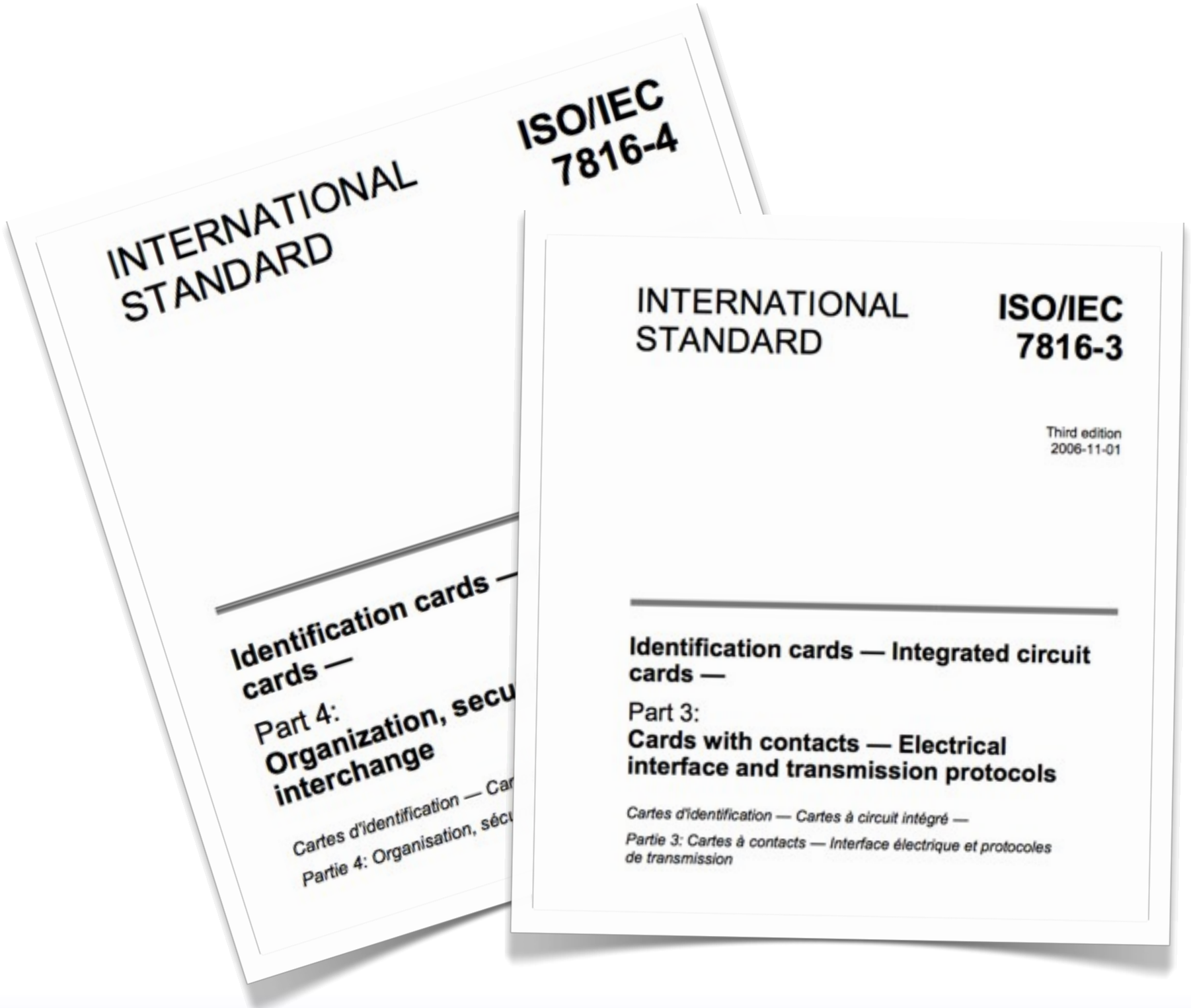
http://www.openscdp.org/scsh3/


VeriFone
Please Insert Card
Menu
Stop
Corr
OK

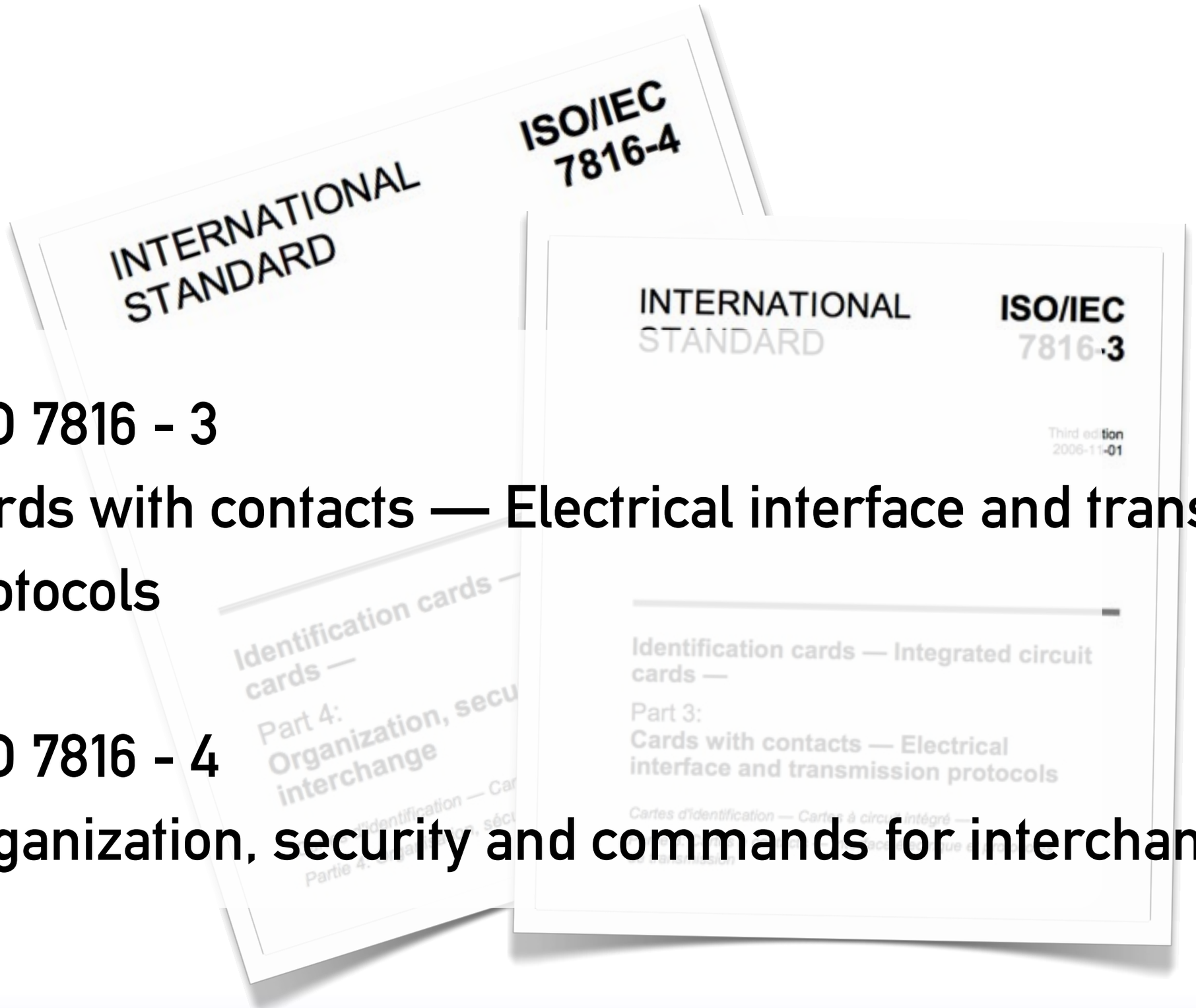

Please Insert Card
4GB
120x
Compact
FlashCard
extreme memory
takeMS
VERSICHERTEN KARTE

shell demo readers

Specifications: ISO 7816



Specifications: ISO 7816



ISO 7816 - 3

Cards with contacts — Electrical interface and transmission protocols

ISO 7816 - 4

Organization, security and commands for interchange

ATR - Answer to Reset describes physical card characteristics

“historical bytes”

Saturday, December 29, 12

Specifications: ISO 7816

Weird (sortof) Filesystem: ignore

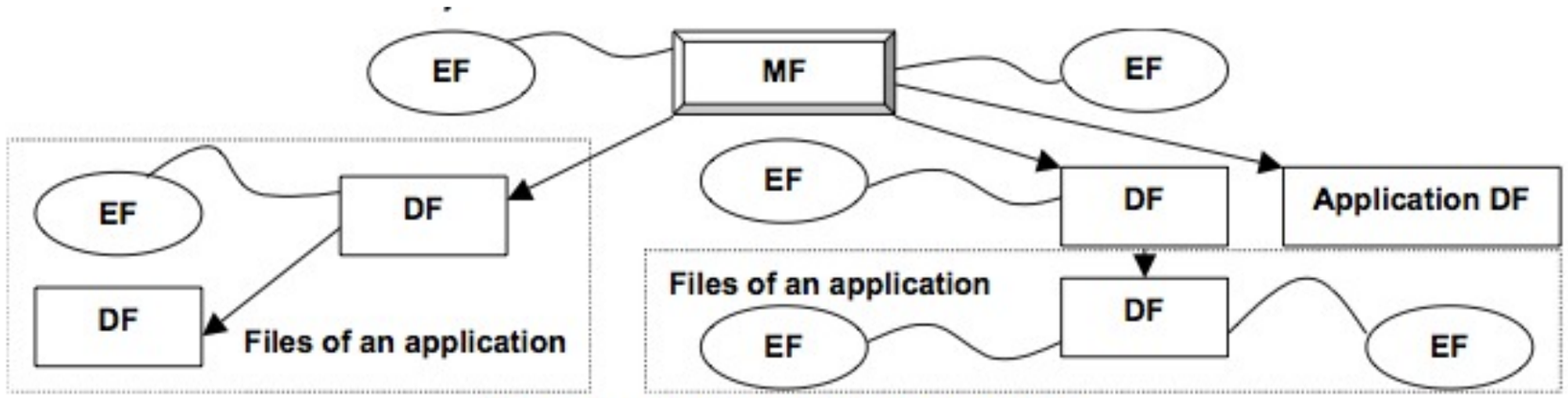


Figure 2 — Example of hierarchy of DFs

— Figure 3 illustrates application DFs in parallel, with no MF seen at the interface, i.e., without any apparent hierarchy of DFs. Such an organization supports independent applications in the card where any application DF may have its own hierarchy of DFs with its corresponding security architecture.

Application DF	**Application DF**	**Files of an application**	**Application DF**

Specifications: ISO 7816

APDU: Application Protocol Data Unit

❧

CLA | INS | P1 | P2 | Lc | Data | Le

Just a bunch of bytes (!)

Specifications: ISO 7816

APDU: Application Protocol Data Unit

❧

CLA | INS | P1 | P2 | Lc | Data | Le

Example:

SELECT

00 | A4 | 04 | 00 | 07 | A0 00 00 00 03 10 10

Specifications: ISO 7816

APDU: Application Protocol Data Unit

❧

CLA | INS | P1 | P2 | Lc | Data | Le

Example:

SELECT

00 | A4 | 04 | 00 | 07 | A0 00 00 00 03 10 10

Specifications: ISO 7816

APDU: Application Protocol Data Unit

❧

CLA | INS | P1 | P2 | Lc | Data | Le

Example:

SELECT

00 | A4 | 04 | 00 | 07 | A0 00 00 00 03 10 10

Specifications: ISO 7816

APDU: Application Protocol Data Unit

❧

CLA | INS | P1 | P2 | Lc | Data | Le

Example:

SELECT

00 | A4 | 04 | 00 | 07 | A0 00 00 00 03 10 10

Specifications: ISO 7816

APDU: Application Protocol Data Unit

❧

CLA | INS | P1 | P2 | Lc | Data | Le

Example:

SELECT

00 | A4 | 04 | 00 | 07 | A0 00 00 00 03 10 10

Specifications: ISO 7816

APDU: Application Protocol Data Unit

❧

CLA | INS | P1 | P2 | Lc | Data | Le

Example:

SELECT

00 | A4 | 04 | 00 | 07 | A0 00 00 00 03 10 10

Specifications: ISO 7816

T=0 vs. T=1

❧

Low Level Communication

UART

character vs. block

Specifications: ISO 7816

T=0 vs. T=1

❧

What you need to know:

T=0 can't send and receive data in one APDU

Difference doesn't matter.

Specifications: ISO 7816

T=0 vs. ~~T=1~~

What you need to know:

T=0 can't send and receive data in one APDU

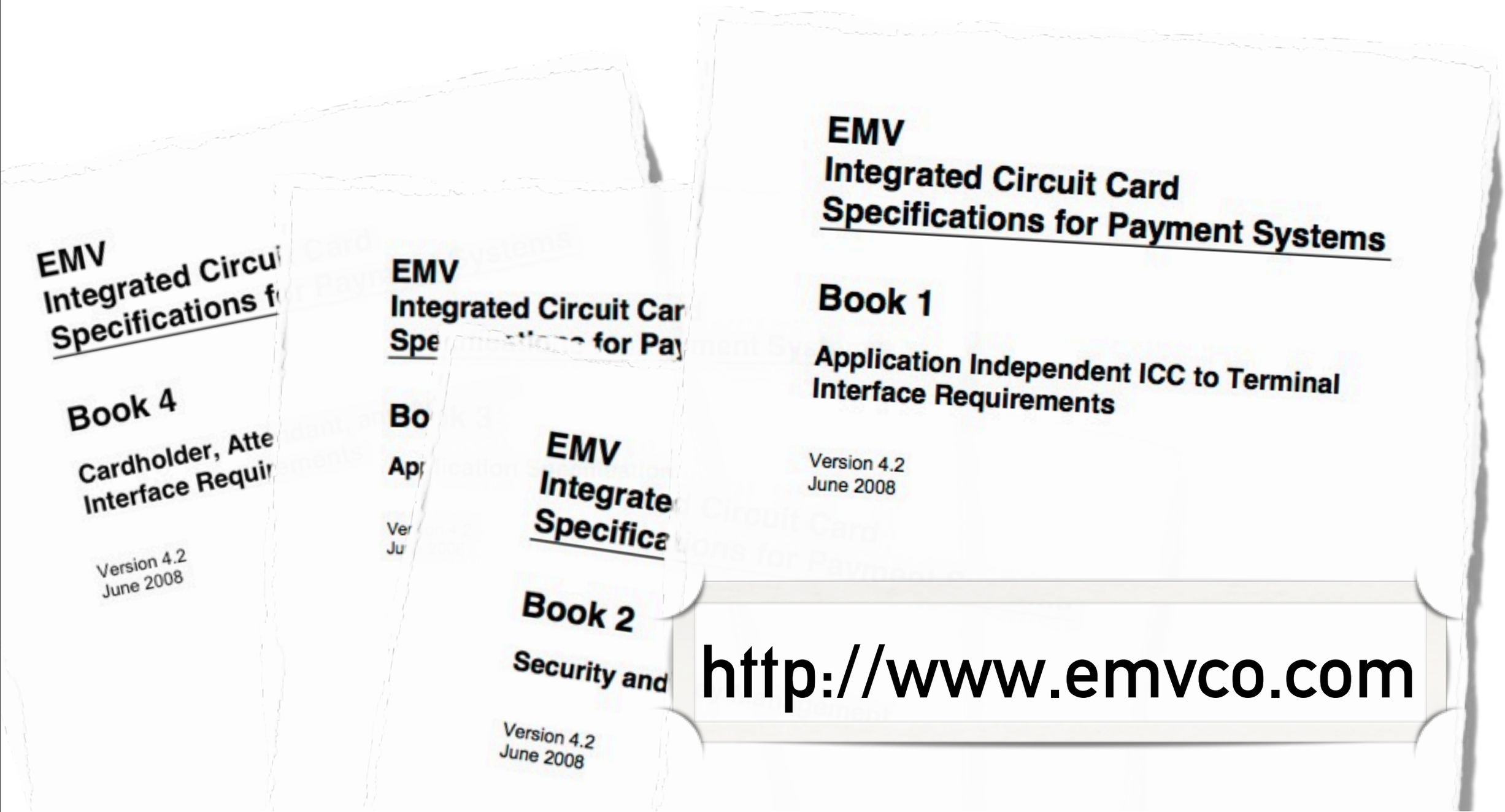
Difference doesn't matter.

Nobody uses T=1

demo SELECT

Specifications: EMV

Books 1, 2, 3 & 4; CPS & CPA

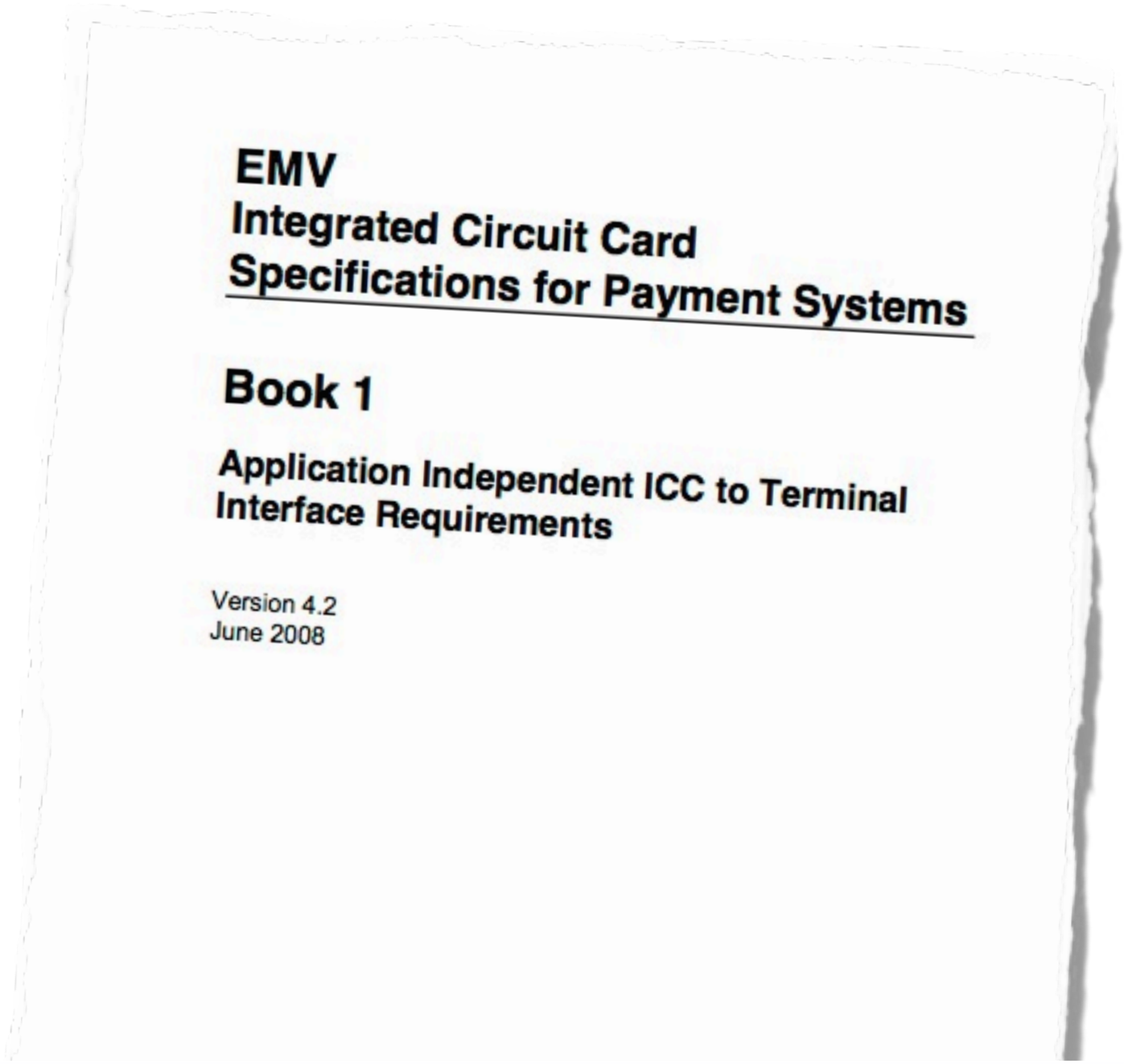


Tim Becker tim@kuriositaet.de @a28002767 www.anykey0x.de

Specifications: EMV

Book 1

Basics, Review of ISO 7816 3&4


EMV
Integrated Circuit Card
Specifications for Payment Systems

Book 1

Application Independent ICC to Terminal
Interface Requirements

Version 4.2
June 2008

Tim Becker tim@kuriositaet.de @a28002767

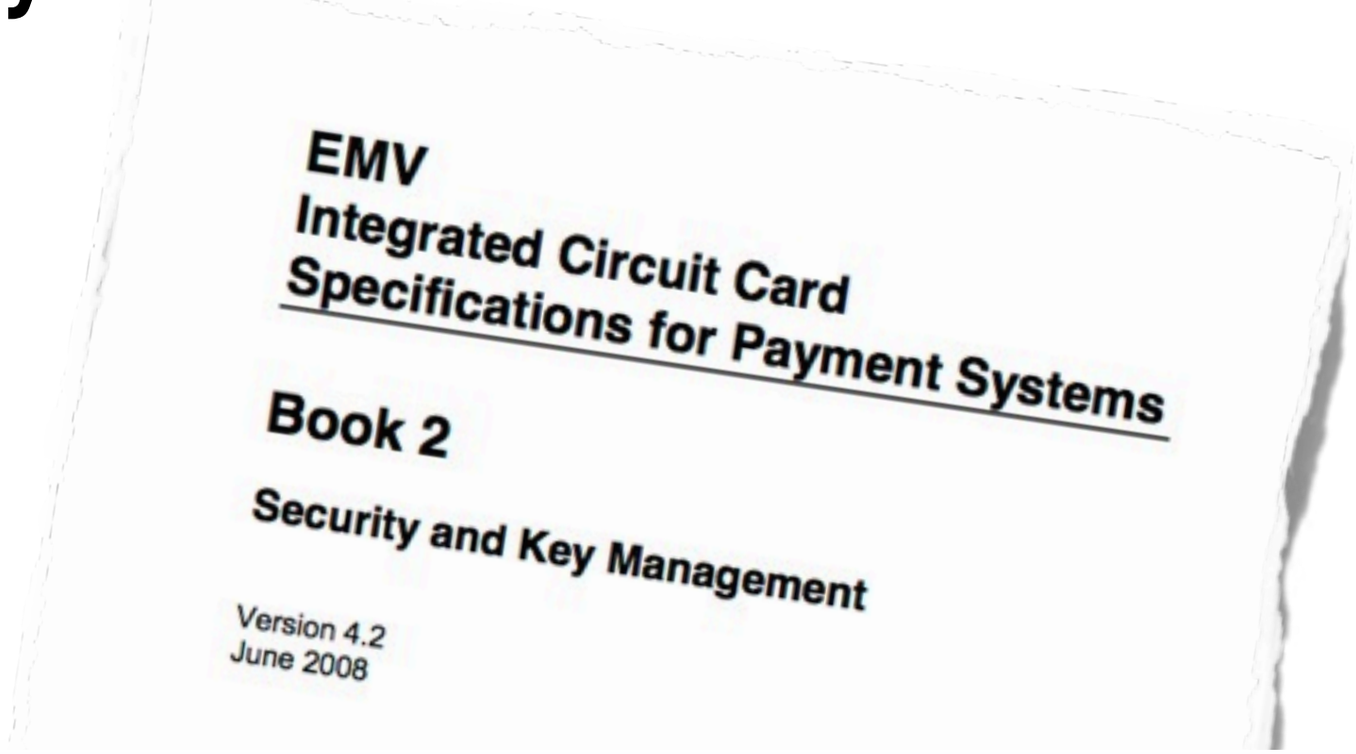
Specifications: EMV

Book 2

Security and Key Management:

Cryptograms & Certificates (not x.509!)

Keys & Key Derivation


EMV
Integrated Circuit Card
Specifications for Payment Systems

Book 2

Security and Key Management

Version 4.2
June 2008

Tim Becker tim@kuriositaet.de @a28002767 www.anykey0x.de

Specifications: EMV

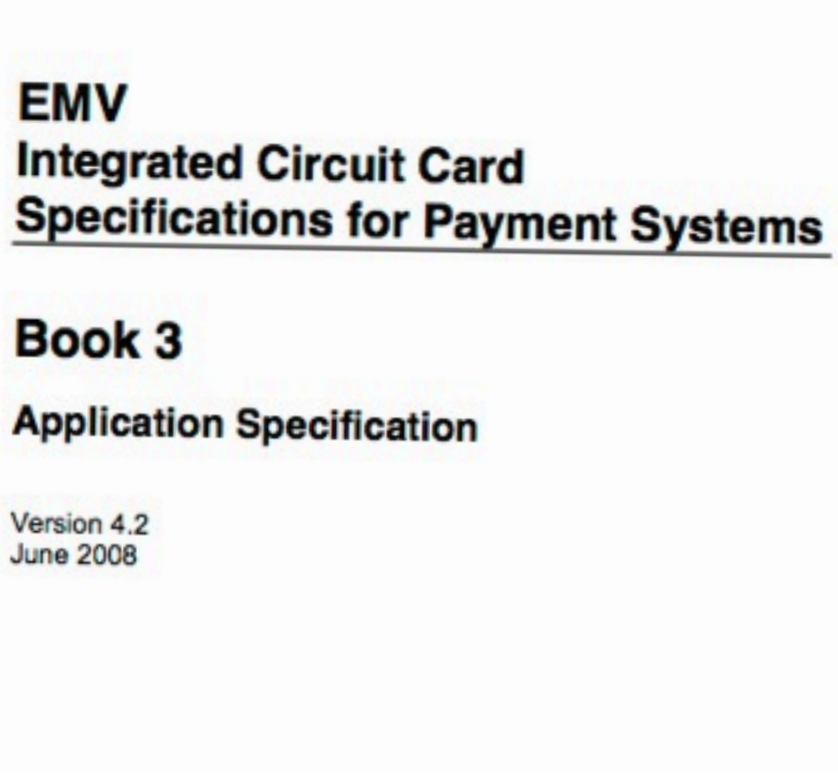
Book 3

Application Specification:

Most Important!

EMV APDUs & Functionality

Data Dictionary ❤



EMV
Integrated Circuit Card
Specifications for Payment Systems

Book 3

Application Specification

Version 4.2
June 2008

Tim Becker tim@kuriositaet.de @a28002767

www.anykey0x.de

Specifications: X.690


INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.690
(07/2002)

SERIES X: DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

OSI networking and system aspects – Abstract Syntax Notation One (ASN.1)

Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

ITU-T Recommendation X.690

ASN.1

everything is TLV (BER)

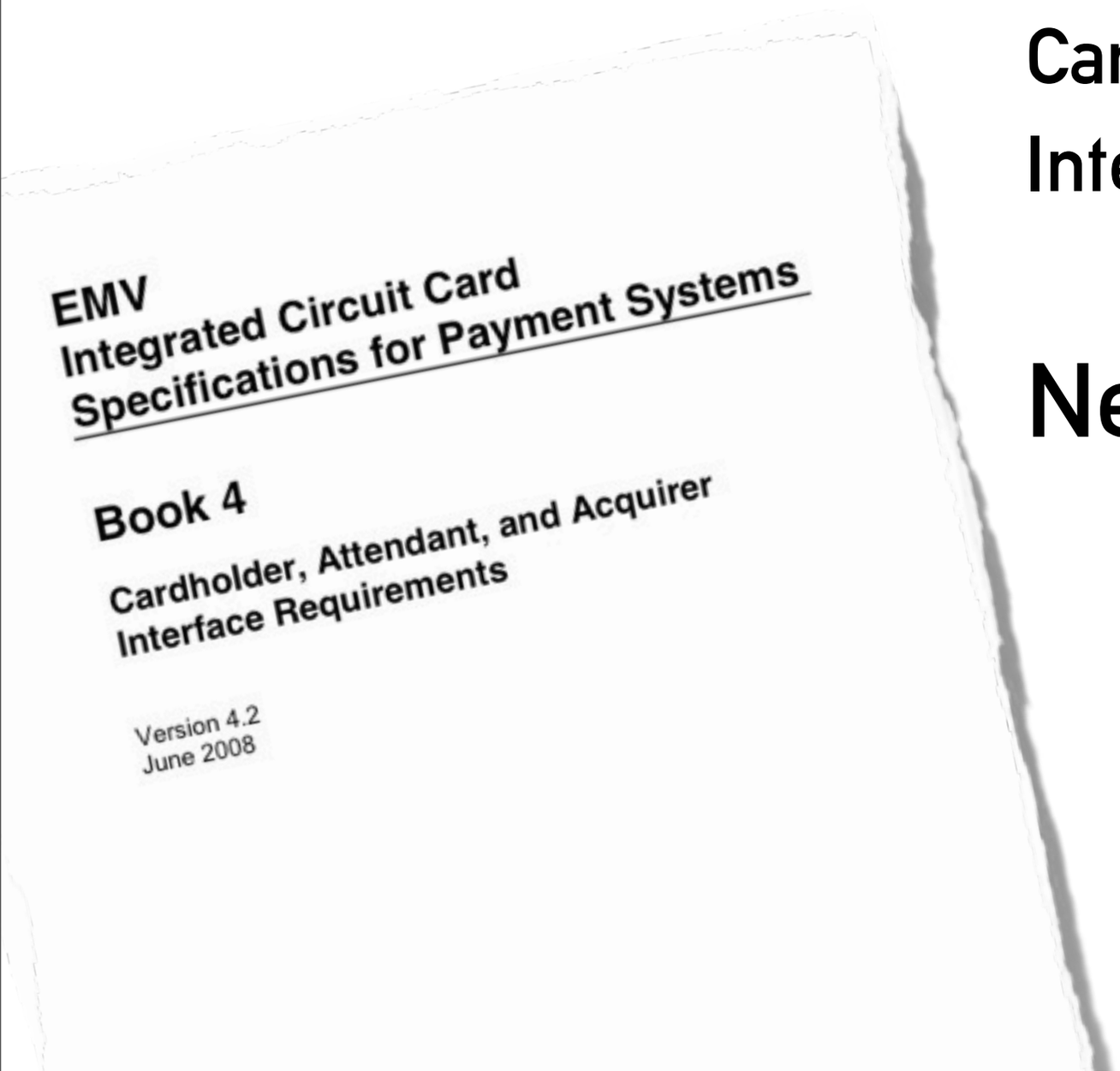
remember the the Data Dictionary in EMV Book 2!

http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf

Tim Becker tim@kuriositaet.de @a28002767 www.anykey0x.de

Specifications: EMV

Book 4



Cardholder, Attendant & Acquirer Interface Requirements

Never used it.

Tim Becker tim@kuriositaet.de @a28002767 www.anykey0x.de

Specifications: EMV

CPS Common Personalization Specification

❧

Industry Standard describing how data is personalized onto the card.

Provides some useful insight into how data is arranged.

Tim Becker tim@kuriositaet.de @a28002767 www.anykey0x.de

Specifications: EMV

CPA Common Payment Application

❧

Books 1-4 describe a “Framework” to create payment applications

CPA describes a concrete implementation

(CCD)

Tim Becker tim@kuriositaet.de @a28002767 www.anykey0x.de

Specifications: M/Chip & VSDC

proprietary
not publicly available except from
Chinese PDF sharing sites.

https://technologypartner.visa.com/Library/Specifications.aspx

Tim Becker tim@kuriositaet.de @a28002767 www.anykey0x.de

Flow

Shake Hands.

Worst first date ever.

Confirm data.

Confirm cardholder.

Seal the deal.

demo: select VSDC, GET PO

Flow

Shake Hands.

Worst first date ever.

Confirm data.

Confirm cardholder.

Seal the deal.

GET PROCESSING OPTIONS

→ PDOL data

← AIP | AFL

AIP | AFL

- **Format 1:** The data object returned in the response message is a primitive data object with tag equal to '80'. The value field consists of the concatenation without delimiters (tag and length) of the value fields of the AIP and the AFL. The coding of the data object returned in the response message is shown in Figure 4:

'80'	Length	Application Interchange Profile	Application File Locator

AIP | AFL

'80'	Length	Application Interchange Profile	Application File Locator

5c00080101001001030018010201

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	x	x	x	x	x	x	x	RFU
x	1	x	x	x	x	x	x	SDA supported
x	x	1	x	x	x	x	x	DDA supported
x	x	x	1	x	x	x	x	Cardholder verification is supported
x	x	x	x	1	x	x	x	Terminal risk management is to be performed
x	x	x	x	x	1	x	x	Issuer authentication is supported [20]
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	1	CDA supported

AIP | AFL

'80'	Length	Application Interchange Profile	Application File Locator

5c00080101001001030018010201

list of 4 byte entries indicating what data to read from the card

AIP | AFL

'80'	Length	Application Interchange Profile	Application File Locator

08010100100103001801020 1

list of 4 byte entries indicating what data to read from the card

AIP | AFL

'80'	Length	Application Interchange Profile	Application File Locator

08010100100103001801020 1

five most significant bits of the first byte indicate the SFI

AIP | AFL

'80'	Length	Application Interchange Profile	Application File Locator

08010100**10010300**18010201

five most significant bits of the first byte indicate the SFI

0x08	0000 1000	1
0x10	0001 0000	2
0x18	0001 1000	3

AIP | AFL

'80'	Length	Application Interchange Profile	Application File Locator

08010100**10010300**18010201

the second byte indicates the first (or only) record number to be read for that SFI.

0x01	start reading at record #1

AIP | AFL

'80'	Length	Application Interchange Profile	Application File Locator

08010100**10010300**18010201

the third byte indicates the last record number to be read for that SFI

SFI # 1	from rec # 1	to rec # 1
SFI # 2	from rec # 1	to rec # 3
SFI # 3	from rec # 1	to rec # 2

AIP | AFL

'80'	Length	Application Interchange Profile	Application File Locator

08010100**10010300**18010201

the fourth byte indicates the number of records involved in offline data authentication starting with the record number coded in the second byte.

AIP | AFL

'80'	Length	Application Interchange Profile	Application File Locator

08010100100103000180102 01

the fourth byte indicates the number of records involved in offline data authentication starting with the record number coded in the second byte.

demo READ RECORD

Service Code

Table 3 — Service code assignments

Value	Position 1		Position 2	Position 3	
	Interchange	Technology	Authorization processing	Allowed services	PIN requirements
0	—	—	Normal [e]	No restrictions	PIN required
1	International [a]	—	—	No restrictions	—
2	International [a]	Integrated circuit card [b]	By issuer [f]	Goods and services only	—
3	—	—	—	ATM only	PIN required
4	—	—	By issuer [f] unless explicit bilateral agreement applies	Cash only	—
5	National [c]	—	—	Goods and services only	PIN required
6	National [c]	Integrated circuit card [b]	—	No restrictions	Prompt for PIN if PED present [g]
7	Private [d]	—	—	Goods and services only	Prompt for PIN if PED present [g]
8	—	—	—	—	—
9	Test	—	—	—	—
NOTE	All undefined values are reserved for future use by ISO.				

ISO 7813 §7.5

Service Code

Table 3 — Service code assignments

Value	Position 1		Position 2	Position 3	
	Interchange	Technology	Authorization	Allowed services	PIN requirements
0	—	—	Normal [e]	No restrictions	PIN required
1	International [a]	—		No restrictions	—
2	International [a]	Integrated circuit card [b]	By issuer [f]	Goods and services only	—
3	—	—	—	ATM only	PIN required
4	—	—	By issuer [f] unless explicit bilateral agreement applies	Cash only	—
5	National [c]	—	—	Goods and services only	PIN required
6	National [c]	Integrated circuit card [b]	—	No restrictions	Prompt for PIN if PED present [g]
7	Private [d]	—	—	Goods and services only	Prompt for PIN if PED present [g]
8	—	—	—	—	—
9	Test	—	—	—	—
NOTE	All undefined values are reserved for future use by ISO.				

ISO 7813 §7.5

Application Usage Control

The Application Usage Control indicates restrictions limiting the application geographically or to certain types of transactions.

EMV Book 3 §10.4.2

Application Usage Control

ff80

Application Usage Control Byte 1 (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Valid for domestic cash transactions
x	1	x	x	x	x	x	x	Valid for international cash transactions
x	x	1	x	x	x	x	x	Valid for domestic goods
x	x	x	1	x	x	x	x	Valid for international goods
x	x	x	x	1	x	x	x	Valid for domestic services
x	x	x	x	x	1	x	x	Valid for international services
x	x	x	x	x	x	1	x	Valid at ATMs
x	x	x	x	x	x	x	1	Valid at terminals other than ATMs

EMV Book 3 Annex C2

Application Usage Control

ff80

Application Usage Control Byte 2 (Rightmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Domestic cashback allowed
x	1	x	x	x	x	x	x	International cashback allowed
x	x	0	x	x	x	x	x	RFU
x	x	x	0	x	x	x	x	RFU
x	x	x	x	0	x	x	x	RFU
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

EMV Book 3 Annex C2

CVM List

00000000**00000000**01031e0302031f00

Amount 1 & 2

seldom used, ignore.

CVM List

000000000000000000**0103**1e**03**02**03**1f**00**

A variable-length list of two-byte data elements called Cardholder Verification Rules (CV Rules)

EMV Book 3 §10.5

CVM List

0000000000000000000103 1e03 02 03 1f00

Each CV Rule describes a CVM and the conditions under which that CVM should be applied

EMV Book 3 §10.5

CVM List

00000000000000000**0103** **1e03** **0203** **1f00**

“01”	Plaintext PIN verification performed by ICC
“1e”	Signature (paper)
“02”	Enciphered PIN verified online
“1f”	No CVM required

EMV Book 3 Annex C3

CVM List

0000000000000000**0103** **1e03** **0203** **1f00**

Each CV Rule describes a CVM and the conditions under which that CVM should be applied

EMV Book 3 §10.5

CVM List

000000000000000000**0103**1e**03**02**03**1f**00**

Each CV Rule describes a CVM and the conditions under which that CVM should be applied

“03”	If terminal supports the CVM
“00”	Always

EMV Book 3 Annex C3

Issuer Action Code(s)

IAC Default	f040008800
IAC Denial	0010000000
IAC Online	f040009800

EMV Book 3 Annex C5

TVR Byte 1: (Leftmost)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Offline data authentication was not performed
x	1	x	x	x	x	x	x	SDA failed
x	x	1	x	x	x	x	x	ICC data missing
x	x	x	1	x	x	x	x	Card appears on terminal exception file [23]
x	x	x	x	1	x	x	x	DDA failed
x	x	x	x	x	1	x	x	CDA failed
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

TVR Byte 2:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	ICC and terminal have different application versions
x	1	x	x	x	x	x	x	Expired application
x	x	1	x	x	x	x	x	Application not yet effective
x	x	x	1	x	x	x	x	Requested service not allowed for card product
x	x	x	x	1	x	x	x	New card
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

EMV Book 3 Annex C5

TVR Byte 3:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Cardholder verification was not successful
x	1	x	x	x	x	x	x	Unrecognised CVM
x	x	1	x	x	x	x	x	PIN Try Limit exceeded
x	x	x	1	x	x	x	x	PIN entry required and PIN pad not present or not working
x	x	x	x	1	x	x	x	PIN entry required, PIN pad present, but PIN was not entered
x	x	x	x	x	1	x	x	Online PIN entered
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

TVR Byte 4:

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	x	x	x	x	x	x	Transaction exceeds floor limit
x	1	x	x	x	x	x	x	Lower consecutive offline limit exceeded
x	x	1	x	x	x	x	x	Upper consecutive offline limit exceeded
x	x	x	1	x	x	x	x	Transaction selected randomly for online processing
x	x	x	x	1	x	x	x	Merchant forced transaction online
x	x	x	x	x	0	x	x	RFU
x	x	x	x	x	x	0	x	RFU
x	x	x	x	x	x	x	0	RFU

EMV Book 3 Annex C5

Shake Hands.

Worst first date ever.

Confirm data.

Confirm cardholder.

Seal the deal.

demo cert

Getting the Issuer's Public Key

Scheme CA certs are bootstrapped in terminal identified by [Certification Authority Public Key Index] on card

Issuer Cert^{CA} is on card, contains part of Issuer Modulus, combined with the [Issuer Public Key Remainder]

EMV Book 2 §6.3

Field Name	Length	Description	Format
Recovered Data Header	1	Hex value '6A'	b
Certificate Format	1	Hex value '02'	b
Issuer Identifier	4	Leftmost 3-8 digits from the PAN (padded to the right with Hex 'F's)	cn 8
Certificate Expiration Date	2	MMYY after which this certificate is invalid	n 4
Certificate Serial Number	3	Binary number unique to this certificate assigned by the certification authority	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme [15]	b
Issuer Public Key Algorithm Indicator	1	Identifies the digital signature algorithm to be used with the Issuer Public Key [15]	b
Issuer Public Key Length	1	Identifies the length of the Issuer Public Key Modulus in bytes	b
Issuer Public Key Exponent Length	1	Identifies the length of the Issuer Public Key Exponent in bytes	b
Issuer Public Key or Leftmost Digits of the Issuer Public Key	N_{CA} – 36	If $N_I \leq N_{CA} - 36$, consists of the full Issuer Public Key padded to the right with $N_{CA} - 36 - N_I$ bytes of value 'BB' If $N_I > N_{CA} - 36$, consists of the $N_{CA} - 36$ most significant bytes of the Issuer Public Key [16]	b
Hash Result	20	Hash of the Issuer Public Key and its related information	b
Recovered Data Trailer	1	Hex value 'BC'	b

Getting the Issuer's Public Key

Header

Expiration Date

```
6a 02 47 61 73 ff 12 30    00 02 90 01 01 70 01 bd
ba db 8e c4 f4 89 c0 d6    0e 14 63 2c ce aa 41 c8
df d1 2e cf 36 51 db 4c    84 7d ba 8c 75 5d 6e 2f
46 2c fd 99 e1 75 61 ee    6e 6a c6 0f 31 58 57 90
c6 f9 5f 06 5e 7d 2a 2c    73 19 07 0b fc b9 44 8b
51 27 b6 c9 09 63 de 7f    62 11 fd 34 eb aa 00 47
50 62 81 47 a8 d4 db 9a    a9 0d a8 16 de a9 8a 99
8f 2f 96 ee a5 79 30 88    b0 e4 f5 7c 06 fb 86 bc
```

Trailer

Getting the Issuer's Public Key

```
6a 02 47 61 73 ff 12 30    00 02 90 01 01 70 01 [bd
ba db 8e c4 f4 89 c0 d6    0e 14 63 2c ce aa 41 c8
df d1 2e cf 36 51 db 4c    84 7d ba 8c 75 5d 6e 2f
46 2c fd 99 e1 75 61 ee    6e 6a c6 0f 31 58 57 90
c6 f9 5f 06 5e 7d 2a 2c    73 19 07 0b fc b9 44 8b
51 27 b6 c9 09 63 de 7f    62 11 fd 34 eb aa 00 47
50 62 81 47 a8 d4 db 9a    a9 0d a8]16 de a9 8a 99
8f 2f 96 ee a5 79 30 88    b0 e4 f5 7c 06 fb 86 bc
```

Leftmost Digits of the Issuer Public Key

Getting the Issuer's Public Key

```
6a 02 47 61 73 ff 12 30    00 02 90 01 01 70 01 bd
ba db 8e c4 f4 89 c0 d6    0e 14 63 2c ce aa 41 c8
df d1 2e cf 36 51 db 4c    84 7d ba 8c 75 5d 6e 2f
46 2c fd 99 e1 75 61 ee    6e 6a c6 0f 31 58 57 90
c6 f9 5f 06 5e 7d 2a 2c    73 19 07 0b fc b9 44 8b
51 27 b6 c9 09 63 de 7f    62 11 fd 34 eb aa 00 47
50 62 81 47 a8 d4 db 9a    a9 0d a8 16 de a9 8a 99
8f 2f 96 ee a5 79 30 88    b0 e4 f5 7c 06 fb 86 bc
```

SHA1 Hash of Issuer PK Data

Issuer Cert^{CA} is on card,

contains part of Issuer Modulus, combined with the [Issuer Public Key Remainder]

SDA Cert^{Issuer} contains a hash of data to be verified

Field Name	Length	Description	Format
Recovered Data Header	1	Hex value '6A'	b
Signed Data Format	1	Hex value '03'	b
Hash Algorithm Indicator	1	Identifies the hash algorithm used to produce the Hash Result in the digital signature scheme [8]	b
Data Authentication Code	2	Issuer-assigned code	b
Pad Pattern	$N_I - 26$	Pad pattern consisting of $N_I - 26$ bytes of value 'BB' [9]	b
Hash Result	20	Hash of the Static Application Data to be authenticated	b
Recovered Data Trailer	1	Hex Value 'BC'	b

Signed Data Format

Padding

```
6a 03 01 da c5 bb bb bb    bb bb bb bb bb bb bb bb
bb bb bb bb bb bb bb bb    bb bb bb bb bb bb bb bb
bb bb bb bb bb bb bb bb    bb bb bb bb bb bb bb bb
bb bb bb bb bb bb bb bb    bb bb bb bb bb bb bb bb
bb bb bb bb bb bb bb bb    bb bb bb bb bb bb bb bb
bb bb bb bb bb bb bb bb    bb bb bb [99 d7 b7 55 50
aa fc fb 90 67 21 96 ad    79 a6 f4 6f 37 25 3b] bc
```

SHA1 hash of signed data
(remember the AFL?)

Issuer Cert^{CA} is on card,

contains part of Issuer Modulus, combined with the [Issuer Public Key Remainder]

ICC PK Cert^{Issuer} contains card's PK (if DDA/CDA supported)

ICC PIN PK Cert^{Issuer}

contains key for PIN encipherment (optional)

DDA: dynamic data authentication

sign random challenge
(DDOL) provided by terminal
with ICC private key using the
INTERNAL AUTHENTICATE command

Shake Hands.

Worst first date ever.

Confirm data.

Confirm cardholder.

Seal the deal.

demo VERIFY

Shake Hands.

Worst first date ever.

Confirm data.

Confirm cardholder.

Seal the deal.

CDOL1

9f 02 06 9f 03 06 9f 1a 02 95 05 5f 2a 02 9a 03 9c 01 9f 37 04

9f 02	06	Amount, Authorised (Numeric)
9f 03	06	Amount, Other (Numeric)
9f 1a	02	Terminal Country Code
95	05	Terminal Verification Results
5f 2a	02	Transaction Currency Code
9a	03	Transaction Date
9c	01	Transaction Type
9f 37	04	Unpredictable Number

Type	Abbreviation	Meaning
Application Authentication Cryptogram	AAC	Transaction declined
Authorisation Request Cryptogram	ARQC	Online authorisation requested
Transaction Certificate	TC	Transaction approved

EMV Book 3 §6.5.5.1

80 00 03 8d e6 d3 fd f1 f1 d9 5b 06 01 0a 03 a4 10 00

Value	Presence
Cryptogram Information Data (CID)	M
Application Transaction Counter (ATC)	M
Application Cryptogram (AC)	M
Issuer Application Data (IAD)	O

EMV Book 3 §6.5.5.4

CID

Cryptogram

IAD including CVR

80 00 03 8d e6 d3 fd f1 f1 d9 5b 06 01 0a 03 a4 10 00

ATC

Value	Presence
Cryptogram Information Data (CID)	M
Application Transaction Counter (ATC)	M
Application Cryptogram (AC)	M
Issuer Application Data (IAD)	O

EMV Book 3 §6.5.5.4

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0							AAC
0	1							TC
1	0							ARQC
1	1							RFU
		x	x					Payment System-specific cryptogram
				0				No advice required
				1				Advice required
					x	x	x	Reason/advice code
					0	0	0	No information given
					0	0	1	Service not allowed
					0	1	0	PIN Try Limit exceeded
					0	1	1	Issuer authentication failed
					1	x	x	Other values RFU

EMV Book 3 §6.5.5.4

CDOL2

8a 02 9f 02 06 9f 03 06 9f 1a 02 95 05 5f 2a 02 9a 03 9c 01 9f 37 04

8a	02	Authorisation Response Code
9f 02	06	Amount, Authorised (Numeric)
9f 03	06	Amount, Other (Numeric)
9f 1a	02	Terminal Country Code
95	05	Terminal Verification Results
5f 2a	02	Transaction Currency Code
9a	03	Transaction Date
9c	01	Transaction Type
9f 37	04	Unpredictable Number

CID

IAD including CVR

40 00 03 9e 76 73 7a 43 7b 9e 2d 06 01 0a 03 64 14 00

Value	Presence
Cryptogram Information Data (CID)	M
Application Transaction Counter (ATC)	M
Application Cryptogram (AC)	M
Issuer Application Data (IAD)	O

EMV Book 3 §6.5.5.4

CVR Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x							Application Cryptogram Type Returned in Second GENERATE AC
0	0							AAC
0	1							TC
1	0							Second GENERATE AC Not Requested
1	1							RFU
		x	x					Application Cryptogram Type Returned in First GENERATE AC
		0	0					AAC
		0	1					TC
		1	0					ARQC
		1	1					RFU
				1				CDA Performed
					1			Offline DDA Performed
						1		Issuer Authentication Not Performed
							1	Issuer Authentication Failed

CVR Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					Low Order Nibble of PIN Try Counter
				1				Offline PIN Verification Performed
					1			Offline PIN Verification Performed and PIN Not Successfully Verified
						1		PIN Try Limit Exceeded
							1	Last Online Transaction Not Completed

EMV Book 3 Annex C.7.3 CCD

CVR Byte 3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1								Lower Offline Transaction Count Limit Exceeded
	1							Upper Offline Transaction Count Limit Exceeded
		1						Lower Cumulative Offline Amount Limit Exceeded
			1					Upper Cumulative Offline Amount Limit Exceeded
				1				Issuer-discretionary bit 1
					1			Issuer-discretionary bit 2
						1		Issuer-discretionary bit 3
							1	Issuer-discretionary bit 4

CVR Byte 4

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					Number of Successfully Processed Issuer Script Commands Containing Secure Messaging
				1				Issuer Script Processing Failed
					1			Offline Data Authentication Failed on Previous Transaction
						1		Go Online on Next Transaction Was Set
							1	Unable to go Online

CVR Byte 5

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	RFU

EMV Book 3 Annex C.7.3 CCD

Conclusion

old protocol

widely used

wrong risks mitigated

security by obscurity

reluctance to part with legacy

Thanks!

Questions?

Why are the holes in cat's fur always in the right places for their eyes?