PHILIPS

Philips Information Systems

TB100KIT TRAINNING CARD

Version 3.0 Sept 90

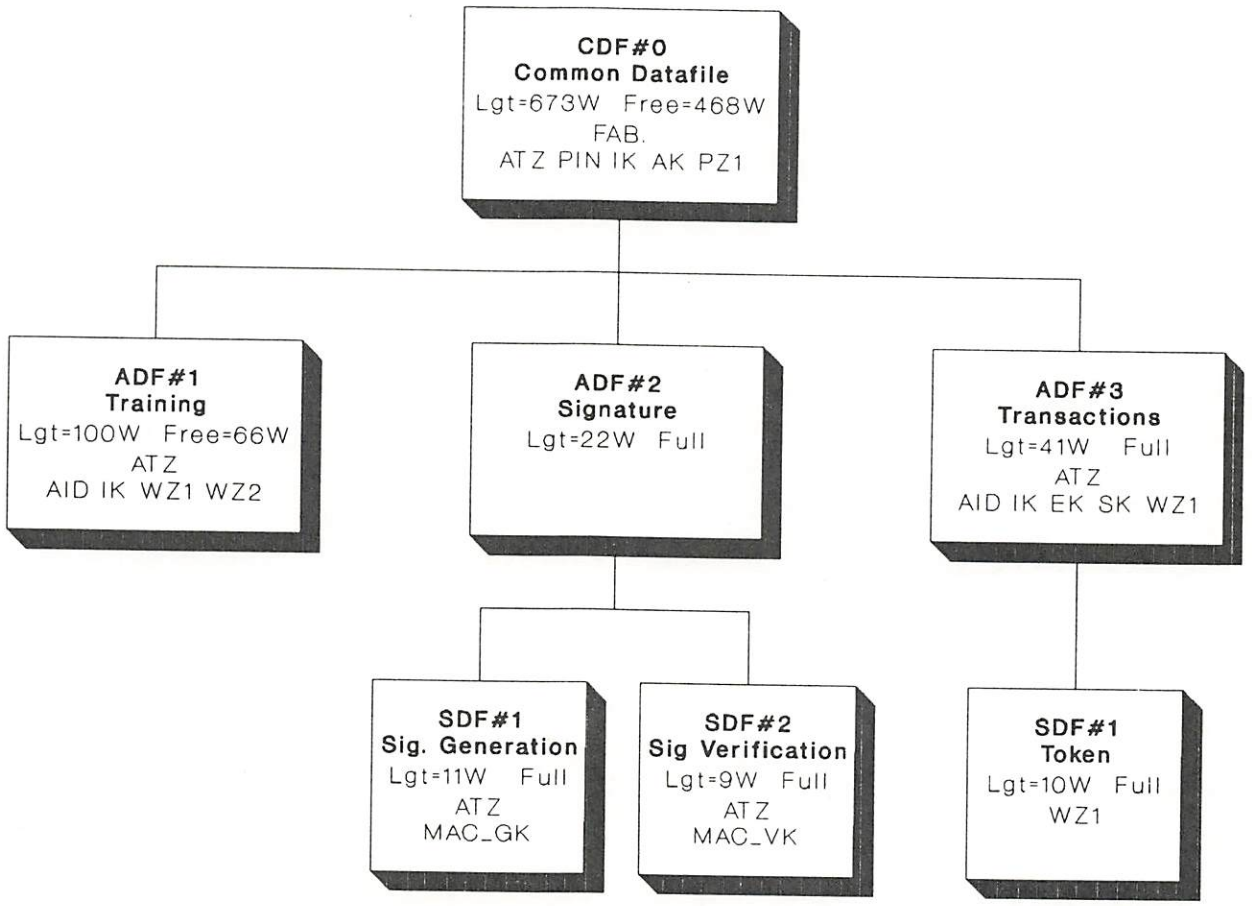
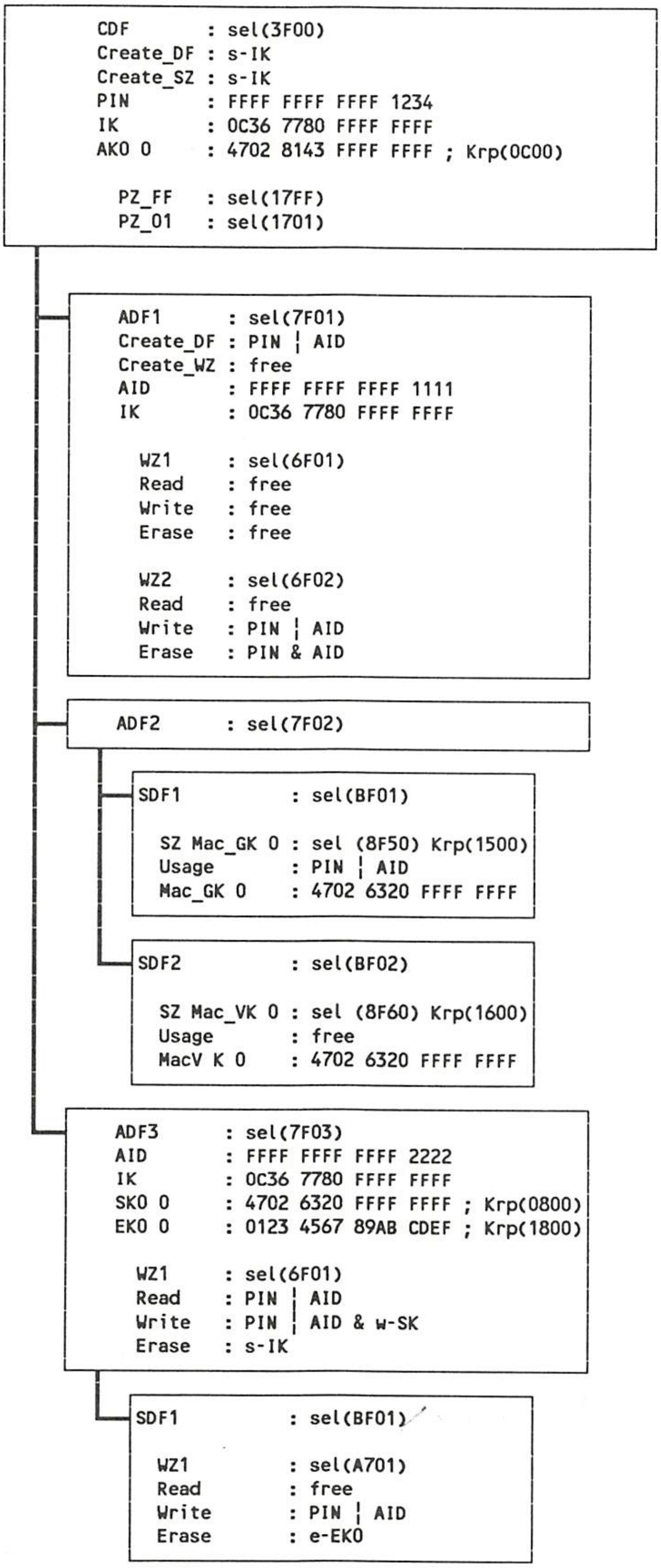


Fig 1: TB100KIT V3.0 Memory Layout

Authors: Christophe Goyet & Bernard Geffrotin

General Overview



```
CDF        : sel(3F00)
Create_DF  : s-IK
Create_SZ  : s-IK
PIN        : FFFF FFFF FFFF 1234
IK         : 0C36 7780 FFFF FFFF
AK0 0      : 4702 8143 FFFF FFFF ; Krp(0C00)

  PZ_FF    : sel(17FF)
  PZ_01    : sel(1701)

    ADF1       : sel(7F01)
    Create_DF  : PIN ¦ AID
    Create_WZ  : free
    AID        : FFFF FFFF FFFF 1111
    IK         : 0C36 7780 FFFF FFFF

      WZ1      : sel(6F01)
      Read     : free
      Write    : free
      Erase    : free

      WZ2      : sel(6F02)
      Read     : free
      Write    : PIN ¦ AID
      Erase    : PIN & AID

    ADF2       : sel(7F02)

        SDF1           : sel(BF01)

          SZ Mac_GK 0  : sel (8F50) Krp(1500)
          Usage        : PIN ¦ AID
          Mac_GK 0     : 4702 6320 FFFF FFFF

        SDF2           : sel(BF02)

          SZ Mac_VK 0  : sel (8F60) Krp(1600)
          Usage        : free
          MacV K 0     : 4702 6320 FFFF FFFF

    ADF3       : sel(7F03)
    AID        : FFFF FFFF FFFF 2222
    IK         : 0C36 7780 FFFF FFFF
    SK0 0      : 4702 6320 FFFF FFFF ; Krp(0800)
    EK0 0      : 0123 4567 89AB CDEF ; Krp(1800)

      WZ1      : sel(6F01)
      Read     : PIN ¦ AID
      Write    : PIN ¦ AID & w-SK
      Erase    : s-IK

        SDF1           : sel(BF01)

          WZ1          : sel(A701)
          Read         : free
          Write        : PIN ¦ AID
          Erase        : e-EK0
```

Description of content

1 CDF: COMMON DATA FILE #0

1.1 CDF Header

Hex value = **3F0002A1 FFEE9EA0**

Level	**CDF**
Reference Number	**00** (HEX)
Length of DF (including header)	02A1 (HEX)
SK to be used for DF creation (if required)	3 (not required)
SK to be used for WZ creation (if required)	3 (not required)
Cardholder conditions for creating a DF	Without protection
Issuer conditions for creating a DF	Authentication by IK
Cardholder conditions for creating a WZ	Without protection
Issuer conditions for creating a WZ	Authentication by IK
Terminal authentication required	NO
DF will be using its own control system	YES
Creation of lower level DF allowed	YES
Invalidation lock (always 1 at creation)	1
Put header in Utilisation Phase	YES

1.2 CDF Content

Type of header or zone/area	Ref. ID or Key vers.	Start Addr.	Stop Addr.	Length of zone in words
Public zone	FF	000	005	006 (6)
ATZ zone	6C	006	008	003 (3)
PIN zone	N/A	009	013	00B (11)
IK zone	0	014	016	003 (3)
AK zone	0	017	019	003 (3)
Public zone	1	01A	028	00F (15)
Data File	1	029	08C	064 (100)
Data File	2	08D	0A2	018 (24)
Data File	3	0A3	0CB	029 (41)
Virgin space	N/A	0CC	29F	1D4 (468)
End of Datafile	N/A	2A0	2A0	001 (1)

1.3 CDF Keys version, type and value

Ref. Id or Key	Version	Type	Value
PIN (1st value)	N/A	N/A	FFFFFFFFFFFF1234
IK	0	N/A	0C367780FFFFFFFF
AK	0	0	47028143FFFFFFFF

PIN Replacement Condition: Submit old PIN (4 changes possible)

1.4 CDF Public zone #FF (Fabrication Zone)

Hex value = 17FF06DA

Level	CDF
Invalidation lock (always 1 at creation)	1
Reference Number	FF (HEX)
Length of Public Zone (including header)	06 (HEX)

This zone, mandatory and written at prepersonalisation time, contains manufacturer information required to compute Manufacturer Key (MK) and Personalisation Key (PK) and unlock the card for personalisation. The values of the keys themselves are stored in the Card System Area ahead of the CDF.

Here is the content of the Fabrication Zone:

8	FABRICATION ZONE HEADER		CHECKSUM	
9	REGISTRATION NUMBER (MSB)		RFU	CTRL
A	REGISTRATION NUMBER (LSB)		RFU	CTRL
B	M.KEY INDEX	ASSEMBLER NUMBER	RFU	KVF M
C	DIVERSIFICATION NUMBER		RFU	CTRL
D	P.KEY INDEX	PERSONALIZATER NUMBER	RFU	KVF P

1.5 CDF Public zone #1

Hex value = 17010FDA

Level	CDF
Invalidation lock (always 1 at creation)	1
Reference Number	01 (HEX)
Length of Public Zone (including header)	0F (HEX)

This zone contains information relating to the card holder (e.g. Name, Address...)

2 ADF #1 TRAINING

2. ADF #1 Header

Hex value = **7F010064 FFBF9ECF**

Level	**ADF**
Reference Number	**01** (HEX)
Length of DF (including header)	0064 (HEX)
SK to be used for DF creation (if required)	3 (not required)
SK to be used for WZ creation (if required)	3 (not required)
Cardholder conditions for creating a DF	Either PIN or AID
Issuer conditions for creating a DF	Without protection
Cardholder conditions for creating a WZ	Without protection
Issuer conditions for creating a WZ	Without protection
Terminal authentication required	NO
DF will be using its own control system	YES
Creation of lower level DF allowed	YES
Invalidation lock (always 1 at creation)	1
Put header in Utilisation Phase	YES

2.2 ADF #1 Content

Type of header or zone/area	Ref. ID or Key vers.	Start Addr.	Stop Addr.	Length of zone in words
ATZ zone	6C	000	002	003 (3)
IK zone	0	003	005	003 (3)
AID zone	N/A	006	008	003 (3)
Working Zone	1	009	014	00C (12)
Working Zone	2	015	020	00C (12)
Virgin space	N/A	021	062	042 (66)
End of Datafile	N/A	063	063	001 (1)

2.3 ADF #1 Keys version, type and value

Ref. ID or Key	Version	Type	Value
AID	N/A	N/A	FFFFFFFFFFFF1111
IK	0	N/A	0C367780FFFFFFFF

No extra room in AID secret zone to allow change of AID.

2.4 ADF #1 Working zone #1

Hex value = 6F01000C F0FFFFA5

Level	ADF
Token mode	NO
Reference Number	**01** (HEX)
Length of **WZ** (including header)	000C (HEX)
Cardholder conditions for erasing	Without protection
Issuer conditions for erasing	Without protection
Number of EK/SK for erasing/writing	0
Number of SK for reading	0
Cardholder conditions for writing	Without protection
Issuer conditions for writing	Without protection
Cardholder conditions for reading	Without protection
Issuer conditions for reading	Without protection
Tracing option	OFF
Invalidation lock (always 1 at creation)	1

2.5 ADF #1 Working zone #2

Hex value = 6F02000C 70BFFF64

Level	ADF
Token mode	NO
Reference Number	**02** (HEX)
Length of **WZ** (including header)	000C (HEX)
Cardholder conditions for erasing	Both PIN and AID
Issuer conditions for erasing	Without protection
Number of EK/SK for erasing/writing	0
Number of SK for reading	0
Cardholder conditions for writing	Either PIN or AID
Issuer conditions for writing	Without protection
Cardholder conditions for reading	Without protection
Issuer conditions for reading	Without protection
Tracing option	OFF
Invalidation lock (always 1 at creation)	1

3 ADF #2 SIGNATURE

3.1 ADF #2 Header

Hex value = **7F020016 FFFFDE9A**

Level	**ADF**
Reference Number	**02** (HEX)
Length of DF (including header)	0016 (HEX)
SK to be used for DF creation (if required)	3 (not required)
SK to be used for WZ creation (if required)	3 (not required)
Cardholder conditions for creating a DF	Without protection
Issuer conditions for creating a DF	Without protection
Cardholder conditions for creating a WZ	Without protection
Issuer conditions for creating a WZ	Without protection
Terminal authentication required	NO
DF will be using its own control system	NO
Creation of lower level DF allowed	YES
Invalidation lock (always 1 at creation)	1
Put header in Utilisation Phase	YES

3.2 ADF #2 Content

Type of header or zone/area	Ref. ID or Key vers.	Start Addr.	Stop Addr.	Length of zone in words
Data File	1	000	00A	00B (11)
Data File	2	00B	013	009 (9)
End of Datafile	N/A	014	014	001 (1)

4 ADF #2_SDF #1 SIGNATURE GENERATION

4.1 ADF #2_SDF #1 Header

Hex value = **BF01000B FFFFBE88**

Level	**SDF**
Reference Number	**01** (HEX)
Length of DF (including header)	000B (HEX)
SK to be used for DF creation (if required)	3 (not required)
SK to be used for WZ creation (if required)	3 (not required)
Cardholder conditions for creating a DF	Without protection
Issuer conditions for creating a DF	Without protection
Cardholder conditions for creating a WZ	Without protection
Issuer conditions for creating a WZ	Without protection
Terminal authentication required	NO
DF will be using its own control system	YES
Creation of lower level DF allowed	NO
Invalidation lock (always 1 at creation)	1
Put header in Utilisation Phase	YES

4.2 ADF #2_SDF #1 Content

Type of header or zone/area	Ref. ID or Key vers.	Start Addr.	Stop Addr.	Length of zone in words
ATZ zone	6C	000	002	003 (3)
MAC. zone	0	003	008	006 (6)
End of Datafile	N/A	009	009	001 (1)

4.3 ADF #2_SDF #1 Keys version, type and value

Ref. ID or Key	Version	Type	Value
MAC_GK	0	N/A	47026320FFFFFFFF

4.4 ADF #2_SDF #1 MAC zone vers #0

Hex value = 8F50061D 01D0FBFF

Level	SDF
Invalidation lock (always 1 at creation)	1
Service of this **MAC.** zone	**Generation** only
MAC. Key version	**0**
Length of MAC. zone.	6
Minimum number of MAC. steps needed	01
Hide the next two words ?	NO
MAC. Initial value	Counter
Position of the mask	RIGHT SIDE
Number of bytes masked in the MAC. result	0
Key needs to be diversified with random ?	NO
Direct load of key is forbidden	NO
Diversification method	ENCRYPTION
Cardholder conditions for MAC.	Either PIN or AID

At personalization, the counter (2words) is initialised to 0

5 ADF #2_SDF #2 SIGNATURE VERIFICATION

5.1 ADF #2_SDF #2 Header

Hex value = **BF020009 FFFFBE87**

Level	**SDF**
Reference Number	**02** (HEX)
Length of DF (including header)	0009 (HEX)
SK to be used for DF creation (if required)	3 (not required)
SK to be used for WZ creation (if required)	3 (not required)
Cardholder conditions for creating a DF	Without protection
Issuer conditions for creating a DF	Without protection
Cardholder conditions for creating a WZ	Without protection
Issuer conditions for creating a WZ	Without protection
Terminal authentication required	NO
DF will be using its own control system	YES
Creation of lower level DF allowed	NO
Invalidation lock (always 1 at creation)	1
Put header in Utilisation Phase	YES

5.2 ADF #2_SDF #2 Content

Type of header or zone/area	Ref. ID or Key vers.	Start Addr.	Stop Addr.	Length of zone in words
ATZ zone	6C	000	002	003 (3)
MAC. zone	0	003	006	004 (4)
End of Datafile	N/A	007	007	001 (1)

5.3 ADF #2_SDF #2 Keys version, type and value

Ref. ID or Key	Version	Type	Value
MAC_VK	0	N/A	47026320FFFFFFFF

5.4 ADF #2_SDF #2 MAC Zone vers #0

Hex value = 8F60040F 01F0FFFF

Level	SDF
Invalidation lock (always 1 at creation)	1
Service of this **MAC.** zone	**Verification** only
MAC. Key version	**0**
Length of MAC. zone.	4
Minimum number of MAC. steps needed	01
Hide the next two words ?	NO
MAC. Initial value	External value
Position of the mask	RIGHT SIDE
Number of bytes masked in the MAC. result	0
Key needs to be diversified with random ?	NO
Direct load of key is forbidden	NO
Diversification method	ENCRYPTION
Cardholder conditions for MAC.	Without protection

6 ADF #3 TRANSACTIONS

6.1 ADF #3 Header

Hex value = **7F030029 FFFF9EC8**

Level	**ADF**
Reference Number	**03** (HEX)
Length of DF (including header)	0029 (HEX)
SK to be used for DF creation (if required)	3 (not required)
SK to be used for WZ creation (if required)	3 (not required)
Cardholder conditions for creating a DF	Without protection
Issuer conditions for creating a DF	Without protection
Cardholder conditions for creating a WZ	Without protection
Issuer conditions for creating a WZ	Without protection
Terminal authentication required	NO
DF will be using its own control system	YES
Creation of lower level DF allowed	YES
Invalidation lock (always 1 at creation)	1
Put header in Utilisation Phase	YES

6.2 ADF #3 Content

Type of header or zone/area	Ref. ID or Key vers.	Start Addr.	Stop Addr.	Length of zone in words
ATZ zone	6C	000	002	003 (3)
AID zone	N/A	003	007	005 (5)
IK zone	0	008	00A	003 (3)
EK zone	0	00B	00D	003 (3)
SK zone	0	00E	010	003 (3)
Working Zone	1	011	01C	00C (12)
Data File	1	01D	026	00A (10)
End of Datafile	N/A	027	027	001 (1)

6.3 ADF #3 Keys version, type and value

Ref. ID or Key	Version	Type	Value
AID (1st Value)	N/A	N/A	FFFFFFFFFFFF2222
IK	0	N/A	0C367780FFFFFFFF
EK	0	0	0123456789ABCDEF
SK	0	0	47026320FFFFFFFF

AID Replacement Condition: Submit old AID **and** Submit IK.

6.4 ADF #3 Working zone #1

Hex value = 6F01000C E09BFF19

Level	ADF
Token mode	NO
Reference Number	**01** (HEX)
Length of **WZ** (including header)	000C (HEX)
Cardholder conditions for erasing	Without protection
Issuer conditions for erasing	Authentication by IK
Number of EK/SK for erasing/writing	0
Number of SK for reading	0
Cardholder conditions for writing	Either PIN or AID
Issuer conditions for writing	Secure write by SK
Cardholder conditions for reading	Either PIN or AID
Issuer conditions for reading	Without protection
Tracing option	OFF
Invalidation lock (always 1 at creation)	1

7 ADF #3_SDF #1 TOKEN

7.1 ADF #3_SDF #1 Header

Hex value = BF01000A FFFFFF48

Level	**SDF**
Reference Number	**01** (HEX)
Length of DF (including header)	000A (HEX)
SK to be used for DF creation (if required)	3 (not required)
SK to be used for WZ creation (if required)	3 (not required)
Cardholder conditions for creating a DF	Without protection
Issuer conditions for creating a DF	Without protection
Cardholder conditions for creating a WZ	Without protection
Issuer conditions for creating a WZ	Without protection
Terminal authentication required	NO
DF will be using its own control system	NO
Creation of lower level DF allowed	NO
Invalidation lock (always 1 at creation)	1
Put header in Utilisation Phase	NO

7.2 ADF #3_SDF #1 Content

Type of header or zone/area	Ref. ID or Key vers.	Start Addr.	Stop Addr.	Length of zone in words
Working Zone	1	000	007	008 (8)
End of Datafile	N/A	008	008	001 (1)

7.3 ADF #3_SDF #1 Working zone token #1

Hex value = A7010008 D0BFFFD1

Level	SDF
Token mode	YES
Reference Number	**01** (HEX)
Length of **WZ** (including header)	0008 (HEX)
Cardholder conditions for erasing	Without protection
Issuer conditions for erasing	Secure erase by EK
Number of EK/SK for erasing/writing	0
Number of SK for reading	0
Cardholder conditions for writing	Either PIN or AID
Issuer conditions for writing	Without protection
Cardholder conditions for reading	Without protection
Issuer conditions for reading	Without protection
Tracing option	OFF
Invalidation lock (always 1 at creation)	1