



TNCOS 用户手册

TCOS User Manual

Version 2.2.0

Aug 10, 2017

Document No. : TNCOS-UM-2.2.0

Confidential Proprietary - DO NOT COPY

Copyright (c) 2017 Tiananxin Technology Limited.

All Rights Reserved



版本历史记录:

版本	作者	日期	描述
V1.0.0	T.	Aug 28, 2016	首版
V2.0.0	T.	Aug 4, 2017	添加密码写保护。NFC 标签在仅写一次模式下，支持验证密码可以重写 NDEF 信息。
V2.1.0	T.	Aug 6, 2017	加入读取 NDEF 应用信息命令, 版本号, 编译日期, 公司名等。
V2.1.1	T.	Aug 8, 2017	为了兼容一些终端软件不支持 NFC Type 4 Tag V2.0 规范, 把 Select 命令去掉需要检测 P2 值, 使 NFC 标签可以接受类似 00 A4 00 XX 02 E1 03 这样的命令。
V2.2.0	T.	Aug 10, 2017	添加多一种模式: PIN Protected。NFC 标签只有工作在密码保护模式下, 才能执行重写 NDEF 信息和修改密码命令



目 录

1	引用标准	4
2	定义和缩略语	5
3	TNCOS综述	6
4	命令	7
4.1	命令汇总表	7
4.2	命令APDU简表	8
4.3	选择应用/文件（Select File）	9
4.4	读二进制数据（Read Binary）	10
4.5	更新二进制数据（Update Binary）	11
4.6	擦除NDEF信息（Erase NDEF）	12
4.7	修改密码（Change PIN）	13
4.8	读应用信息（Read ApplInfo）	14
5	NFC应用	15
5.1	读NFC Forum Type 4 Tag标签信息	15
5.2	写NFC Forum Type 4 Tag标签信息	16
6	修改密码流程演示	17
7	重写NDEF信息流程演示	18
8	附录	19
8.1	NXP TagInfo读基于TNCOS的NFC标签图示	19
8.2	NFC Tags Issue Tools读基于TNCOS的NFC标签图示	20



1 引用标准

- [1] ISO 7816-1 first edition 1998-10-15
Identification cards - Integrated circuit(s) cards with contacts
Part 1: Physical characteristics
- [2] ISO 7816-2 first edition 1999-03-01
Identification cards - Integrated circuit(s) cards with contacts
Part 2: Dimensions and location of the contacts
- [3] ISO 7816-3 second edition 1997-12-15
Identification cards - Integrated circuit(s) cards with contacts
Part 3: Electronic signals and transmission protocols
- [4] ISO 7816-4 first edition 1995-09-01
Amendment 1 1997-12-15
Identification cards - Integrated circuit(s) cards with contacts
Part 4: Interindustry commands for interchange
- [5] Federal Information Processing Standards Publication
1980 December 2, FIPS PUB 81
DES Modes of Operation
- [6] PBOC 第3、4、5、6、7、10部分
JR/T0025.4--2005
- [7] EMV 2000
Integrated Circuit Card
Specification for Payment Systems
Version 4.0 December, 2000
- [8] Visa ICC Specification version 1.4.0 (VIS 1.4.0)
31 October 2001
- [9] GB-T15150-1994 (ISO 8583-1987)
产生报文的银行卡一交换报文规范一金融交易内容
- [10] GBT2659-2000 (ISO 3166-1-1997)
世界各国和地区名称代码
- [11] Type 4 Tag Operation Technical Specification, Version 2.0, 2010-11-18
NFCForum-TS-Type-4-Tag_2.0
- [12] NFC Data Exchange Format (NDEF), Version 1.0, 2006-07-24
NFCForum-TS-NDEF_1.0
- [13] NFC Record Type Definition (RTD) Specification, Version 1.0, 2006-07-24
NFCForum-TS-RTD_1.0
- [14] NFC Text Record Type Definition Technical Specification, Version 1.0, 2006-07-24
NFCForum-TS-RTD_Text_1.0
- [15] NFC URI Record Type Definition Technical Specification, Version 1.0, 2006-07-24
NFCForum-TS-RTD_URI_1.0



2 定义和缩略语

缩略语	定义
CLA	命令类别
INS	命令代码
P1,P2	命令参数 1、命令参数 2
Lc	APDU 命令的数据长度
PCB	协议控制字节 (protocol control byte)
R-block	接收准备数据块
S-block	管理数据块
CRC	循环冗余码校验
NDEF	NFC Data Exchange Format (NFC 数据交换格式)
CC File	Capability Container File(能力容器文件)。CC 文件应该是一个只读 EF 文件，并且 FID 固定为 0xE103
NDEF file	存储 NDEF 数据的具体文件
Proprietary File	专用文件。专用文件是一个 EF 文件。里面保存的数据是专有数据 (proprietary data)。用户自定义的数据放这里
Proprietary File Control TLV	专用文件控制 TLV 记录。一条 TLV 记录占用 8 个字节。
NDEF message	NDEF 信息。一条 NDEF 信息包括一条或多条 NDEF 记录
NDEF record	NDEF 记录。一条 NDEF 记录包含一个有效载荷描述。这个描述是由一个类型，一个长度，一个可选的标识组成的。
FSCI	Frame Size for proximity Card Integer
FSC	Frame Size for proximity Card (卡片接收数据缓冲区大小)
SFGI	Start-up Frame Guard time Integer
SFGT	Start-up Frame Guard Time
FWI	Frame Waiting time Integer
FWT	Frame Waiting Time(帧等待时间)
FWT _{MIN}	Minimum Frame Waiting Time (最小帧等待时间)
FWT _{MAX}	Maximum Frame Waiting Time (最大帧等待时间)
FWT _{TEMP}	temporary Frame Waiting Time (临时帧等待时间)
WTX	Waiting Time eXtension (帧等待时间扩展)
WTXM	Waiting Time eXtension Multiplier (帧等待时间扩展乘数)
FSD	Frame Size for proximity coupling Device(读写器接收数据缓冲区大小)
FSDI	Frame Size for proximity coupling Device Integer



3 TNCOS 综述

TNCOS 是专门为 NFC 应用而设计，产品符合 NFC Forum Type 4 Tag 规范。在 TNCOS 中加入了写保护功能，当校验口令正确时，NFC 标签可以再次被重新写入 NDEF 信息。口令是 8 个字节的长度，口令的初始值是 0x40 0x41 0x42 0x43 0x44 0x45 0x46 0x47。口令是明文校验和修改。

TNCOS 可由生产阶段配置为以下四种工作模式：

- 1、自由读写模式
- 2、只读模式
- 3、仅写一次模式
- 4、密码保护模式

TNCOS 特点：

- 符合 NFC Forum Type 4 Tag 规范
- 符合 ISO14443-1/2/3/4 标准
- 非接触通信速率支持最高 424kbit/s，同时可配置支持 106/212/424kbit/s。
- TNCOS 可由生产阶段设定支持的最高通信速率。

应用场景：

- NFC 手机
- 自动化设备授权
- NFC 安全巡检
- POS 机、ATM 机、读写器、等各种终端的 NFC 测试
- NFC 设备测试
- NFC 应用
- 授权应用（自动化设备授权、软件授权、安卓软件授权）



4 命令

4.1 命令汇总表

CLA (hex)	INS (hex)	意义
00	A4	选择应用/文件 (Select File)
00	B0	读二进制数据 (Read Binary)
00	D6	更新二进制数据 (Update Binary)
80	0E	擦除 NDEF 信息 (Erase NDEF)
80	24	修改密码 (Change PIN)
80	B2	读应用信息 (Read AppInfo)



4.2 命令 APDU 简表

名称	CLA	INS	P1	P2	Lc/Le	CData/RData
Select File	00	A4	04/00	00/0C	Lc=07/02	AID/FID
Read Binary	00	B0	AddrH	AddrL	Le=00...FF	读出的二进制数
Update Binary	00	D6	AddrH	AddrL	Lc=01...FF	待更新二进制数
*Erase NDEF	80	0E	00	00	08	PIN
*Change PIN	80	24	00	00	10	OldPIN NewPIN
*Read ApplInfo	80	B2	9X	00	Le=00	

备注：

- 1、加星号（*）的命令是专用命令，非 NFC 论坛定义的通用命令。
- 2、专用命令的执行，需要先成功执行了选 NFC 应用命令才行。



4.3 选择应用/文件（Select File）

任务	选择 NFC 应用或文件	
条件	无	
输入	CLA	'00'
	INS	'A4'
	P1	'04'
	P2'	'00'
	Lc	AID
输出	无	
备注	Lc=07 时，选择 NFC 应用 Lc=02 时，选择 EF 文件	

例子 1：选择 NFC 应用

CMD_APDU = 00 A4 04 00 07 D2 76 00 00 85 01 01

RSP_APDU = 90 00

例子 2：选择 CC 文件

CMD_APDU = 00 A4 00 0C E1 03

RSP_APDU = 90 00

例子 3：选择 NDEF 文件

CMD_APDU = 00 A4 00 0C E1 04

RSP_APDU = 1C C4 77 CF 90 00



4.4 读二进制数据（Read Binary）

任务	读出 NFC 标签中信息数据。	
条件	需要先成功执行了选择 EF 文件命令。	
输入	CLA	'00'
	INS	'B0'
	P1P2	Offset （取值范围： 0x0000 - 0x7FFF）
	Lc	无
	Data	无
	Le	可变
输出	二进制数据	
备注	可以用来读 CC 文件或者是 NDEF 文件数据。	

例子：

Setp1:

Select NFC AID

CMD_ADPU = 00 A4 04 00 07 D2 76 00 00 85 01 01

RSP_ADPU = 90 00

Setp2: Select CC File

CMD_ADPU = 00 A4 00 0C 02 E1 03

RSP_ADPU = 90 00

Step3: Read CC File

CMD_ADPU = 00 B0 00 00 0F

RSP_ADPU = 00 0F 20 00 80 00 80 04 06 E1 04 00 40 00 00 90 00

Step4: Select NDEF File

CMD_ADPU = 00 A4 00 0C 02 E1 04

RSP_ADPU = 90 00

Step5: Read NLEN field in NDEF File

CMD_ADPU = 00 B0 00 00 02

RSP_ADPU = 00 03 90 00

Step6: Read NDEF message in NDEF File

CMD_ADPU = 00 B0 00 02 13

RSP_ADPU = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 00



4.5 更新二进制数据（Update Binary）

任务	写入新的 NDEF 信息	
条件	需要先选择 NDEF 文件	
输入	CLA	‘00’
	INS	‘D6’
	P1P2	Offset （取值范围：0x0000 - 0x7FFF）
	Lc	可变 （取值范围：0x01 - 0xFF）
	Data	待写入数据
输出	无	
备注	只有 NDEF 文件才可以更新。CC 文件是没法更新的。	

例子：

Setp1:

Select NFC AID

CMD_ADPU = 00 A4 04 00 07 D2 76 00 00 85 01 01

RSP_ADPU = 90 00

Setp2: Select CC File

CMD_ADPU = 00 A4 00 0C 02 E1 03

RSP_ADPU = 90 00

Step3: Read CC File

CMD_ADPU = 00 B0 00 00 0F

RSP_ADPU = 00 0F 20 00 80 00 80 04 06 E1 04 00 40 00 00 90 00

Step4: Select NDEF File

CMD_ADPU = 00 A4 00 0C 02 E1 04

RSP_ADPU = 90 00

Step5: Update Binary in NDEF File

CMD_ADPU = 00 D6 00 02 06 31 32 33 34 35 36

RSP_ADPU = 90 00



4.6 擦除 NDEF 信息（Erase NDEF）

任务	擦除 NDEF 文件信息。实现可以重写 NDEF 信息的功能。	
条件	需要先选择 NDEF 文件	
输入	CLA	'80'
	INS	'0E'
	P1	'00'
	P2	'00'
	Lc	'08'
	Data	PIN
	Le	无
输出	无	
备注	当校验密码正确时，就擦除 NDEF 信息。否则，不能再次重写 NDEF 信息。一旦命令执行成功后，无论是否下电，NFC 标签都可以重写。	

例子：

Setp1:

Select NFC AID

CMD_ADPU = 00 A4 04 00 07 D2 76 00 00 85 01 01

RSP_ADPU = 90 00

Step2: Select NDEF File

CMD_ADPU = 00 A4 00 0C 02 E1 04

RSP_ADPU = 90 00

Step3: Erase NDEF

CMD_ADPU = 80 0E 00 00 08 40 41 42 43 44 45 46 47

RSP_ADPU = 90 00



4.7 修改密码（Change PIN）

任务	修改 NDEF 应用中的密码	
条件	先选择 NDEF 应用	
输入	CLA	'80'
	INS	'24'
	P1	'00'
	P2	'00'
	Lc	'10'
	Data	OldPIN NewPIN
	Le	无
输出	无	
备注	1、知道旧密码才有办法修改密码成功。 2、当修改密码成功后，必须记着新密码，否则影响 NFC 标签部分命令执行。	

例子：

Setp1:

Select NFC AID

CMD_ADPU = 00 A4 04 00 07 D2 76 00 00 85 01 01

RSP_ADPU = 90 00

Step2: Change PIN Command

CMD_ADPU = 80 24 00 00 10 40 41 42 43 44 45 46 47 31 32 33 34 35 36 37 38

RSP_ADPU = 90 00



4.8 读应用信息（Read AppInfo）

任务	读取 NFC 应用信息：包括软件版本号等	
条件	需要先选择 NFC 应用	
输入	CLA	'80'
	INS	'B2'
	P1	'9X'
	P2	'00'
	Lc	无
	Data	无
	Le	'00'
输出	数据 = /*读出的数据流*/	
备注		

例子 1:

Select NFC AID

CMD_ADPU = 00 A4 04 00 07 D2 76 00 00 85 01 01

RSP_ADPU = 90 00

//读应用版本号

CMD_APDU = 80 B2 90 00 00

RSP_APDU = 54 4E 43 4F 53 20 56 32 2E 30 31 90 00

//读日期

CMD_APDU = 80 B2 91 00 00

RSP_APDU = 32 30 31 37 30 38 30 36 90 00

//读公司标识

CMD_APDU = 80 B2 92 00 00

RSP_APDU = 54 49 41 4E 20 41 4E 20 58 49 4E 90 00



5 NFC 应用

5.1 读 NFC Forum Type 4 Tag 标签信息

NFC Forum Type 4 Tag Version 2.0 读标签操作步骤如下：

Resetcard

Setp1: Select NFC AID

CMD_ADPU = 00 A4 04 00 07 D2 76 00 00 85 01 01

RSP_ADPU = 90 00

Setp2: Select CC File

CMD_ADPU = 00 A4 00 0C 02 E1 03

RSP_ADPU = 90 00

Step3: Read CC File

CMD_ADPU = 00 B0 00 00 0F

RSP_ADPU = 90 00

Step4: Select NDEF File

CMD_ADPU = 00 A4 00 0C 02 E1 04

RSP_ADPU = 90 00

Step5: Read NLEN field in NDEF File

CMD_ADPU = 00 B0 00 00 02

RSP_ADPU = 90 00

Step6: Read NDEF message in NDEF File

CMD_ADPU = 00 B0 00 00 00

RSP_ADPU = 90 00



5.2 写 NFC Forum Type 4 Tag 标签信息

NFC Forum Type 4 Tag Version 2.0 标签写入电话号码：13800138000 操作步骤如下：

Resetcard

Setp1: Select NFC AID

CMD_ADPU = 00 A4 04 00 07 D2 76 00 00 85 01 01

RSP_ADPU = 90 00

Setp2: Select CC File

CMD_ADPU = 00 A4 00 0C 02 E1 03

RSP_ADPU = 90 00

Step3: Read CC File

CMD_ADPU = 00 B0 00 00 0F

RSP_ADPU = 00 0F 20 00 80 00 80 04 06 E1 04 00 40 00 00 90 00

Step4: Select NDEF File

CMD_ADPU = 00 A4 00 0C 02 E1 04

RSP_ADPU = 90 00

Step5: Read NLEN field in NDEF File

CMD_ADPU = 00 B0 00 00 02

RSP_ADPU = 00 03 90 00

Step6: Read NDEF message in NDEF File

CMD_ADPU = 00 B0 00 02 13

RSP_ADPU = 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 00

Step7: update NDEF message in NDEF File

CMD_ADPU = 00 D6 00 00 12

RSP_ADPU = 00 10 D1 01 0C 55 05 31 33 38 30 30 31 33 38 30 30 30 90 00

Step8: check content correction

CMD_ADPU = 00 B0 00 00 20

RSP_ADPU = 00 10 D1 01 0C 55 05 31 33 38 30 30 31 33 38 30
30 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 00



6 修改密码流程演示

当 TNCOS 配置为密码保护模式时，是支持修改密码命令的。其他模式则为不支持修改密码操作。

修改密码的操作可以在写 NFC 信息之前，或者是写完 NFC 信息之后进行。通常的做法是先写入 NFC 信息，然后才修改密码操作。成功修改了密码之后，不知道密码的人是没法再次重写 NFC 信息的，只有知道密码的人才能重写 NFC 信息。

步骤 1：按正常操作写入 NFC 信息

步骤 2：执行修改密码命令

Select NFC AID

CMD_ADPU = 00 A4 04 00 07 D2 76 00 00 85 01 01

RSP_ADPU = 90 00

Change PIN Command

CMD_ADPU = 80 24 00 00 10 40 41 42 43 44 45 46 47 31 32 33 34 35 36 37 38

RSP_ADPU = 90 00



7 重写 NDEF 信息流程演示

当TNCOS配置为密码保护模式时，NFC标签是可以重新写入NFC信息的。

例子：

假如 NFC 标签之前已经写入了 NFC 信息，现在需要重写写入新的 NFC 信息--

步骤 1：执行擦除 NDEF 信息命令 (假如密码是：40 41 42 43 44 45 46 47)

CMD_ADPU = 80 0E 00 00 08 40 41 42 43 44 45 46 47

RSP_ADPU = 90 00

步骤 2：执行正常的写入 NDEF 信息流程



8 附录

8.1 NXP TagInfo 读基于 TNCOS 的 NFC 标签图示

参数	Type A			Type B		
	所在域	所在字节	所在位	所在域	所在字节	所在位
FSCI	ATS	T0	低四位	ATQB	ATQB[10]	高四位
DR/DS	ATS	TA1	DR: b2...b0 DS: b6...b4	ATQB	ATQB[9]	DR: b2...b0 DS: b6...b4
SFGI	ATS	TB1	低四位	ATQB	ATQB[12]可选	高四位
FWI	ATS	TB1	高四位	ATQB	ATQB[11]	高四位
NAD	ATS	TC1	b0	ATQB	ATQB[11]	b1
CID	ATS	TC1	b1	ATQB	ATQB[11]	b0



8.2 NFC Tags Issue Tools 读基于 TNCOS 的 NFC 标签图示

NFC Tags Issue Tools 软件是需要配合 Identiv uTrust 4700 F 硬件 NFC 读写器操作的。这种组合可以实现快速读写 NDEF 信息，擦除 NDEF 信息，修改密码等操作。适合工厂，公司快速批量发行 NFC 标签。