NFC TYPE2 标签芯片
F8216SC

技术手册

V1.01

2014.4

上海飞聚电子有限公司

地址：上海市浦东新区张衡路180号1号楼1楼E座

电话：086-021-61683006 传真：086-021-61683005

网址：www.nfcic.com 邮编：201203

Department:	上海飞聚电子有限公司

Security:	Low ☐	Middle ☐	High ■
Priority:	Low ☐	Middle ■	High ☐

Revision	Description	Date	Prepared
V1.01	Initial Release	2013.2	**Mr. Chu**

Review	Signature	Date	Comments

Approval	Signature	Date	Comments

Security Policy:

目 录

1、文件说明

本文档为 NFC 标签芯片 F8216S 的详细技术手册，开发者可基于此文档开发相应的系统，需要更多相关技术文档请联系上海飞聚微电子有限公司。

2、产品特点

2.1 概述

F8216SC 是一款由上海飞聚微电子有限公司研发的，完全支持 NFC Forum Type2 协议和 ISO14443 TypeA 协议的芯片。它除了具有 128 位密钥的三重认证功能外，还具有 96 位真随机数签名映射功能。它可以广泛应用在如商品防伪、身份认证等领域。

2.2 射频接口

- 以无线的方式传输数据和能量
- 完全符合 ISO14443 TYPE A 传输协议
- 工作频率：13.56MHz
- 工作场强:
  - 最小：0.3A/m（标准 ID-1 尺寸天线）
  - 最大：7.5A/m（标准 ID-1 尺寸天线）
- 通信速率：106Kbps
- 数据完整性：16 位 CRC 校验及奇偶检验
- 7 字节 UID，两级防冲突功能

2.3 存储器结构

- 总容量 996 个字节，分为 249 个页，每页 4 个字节
- 用户可用空间 944 个字节，236 页
- 7 个字节的唯一 UID
- 32 位的 OTP 区域，出厂时已做好 NDEF 格式数据的初始化
- 2 个字节的对前 16 个页只读锁存静态锁定区域
- 3 个字节的对 16 页以后区域只读锁存动态锁定区域
- 16 个字节的密钥
- 数据保持时间可达 10 年
- 读写次数可达 10 万次

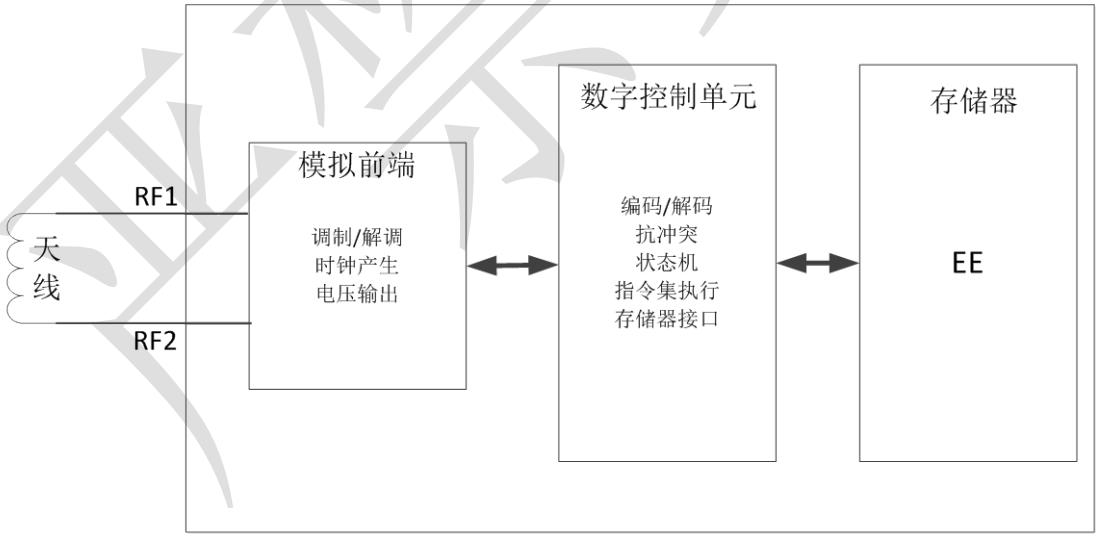
2.4 安全特性

- 7 个字节的唯一 UID
- 数据区只读锁定功能
- 128 位密钥保护
- 96 位真随机数签名映射功能
- 3DES 认证算法，真随机数三重认证
- 密钥暴力攻击失效次数设置功能
- ECC 原始性签名功能

2.5 其它功能特点

- UID ASCII 码映射，可自动序列化 NDEF 格式信息
- 第一个读命令自动触发计数器计数功能
- 计数器值可进行 ASCII 码映射，可作为 NDEF 数据的一部分
- 96 位动态签名值及 UID 可做为 ASCII 码映射，也可作为 NDEF 数据的一部分
- 支持多种外部引脚触发模式等功能
- 支持快速读命令

2.6 结构框图



F8216SC结构框图

3、功能描述

3.1 存储器结构

EE 的存储结构图如下表所示，各区间功能定义见下文所述：

地址	Byte0	Byte1	Byte2	Byte3
00h	SN0	SN1	SN2	BCC0
01h	SN3	SN4	SN5	SN6
02h	BCC1	Internal	Lock0	Lock1
03h	OTP0	OTP1	OTP2	OTP3
04h	User	User	User	User
…	User	User	User	User
…	User	User	User	User
EFh	User	User	User	User
F0h	Lock2	Lock3	Lock4	BDh
F1h	Mirror_Byte	Rcnt_ascii	Mirror_Page	Auth0
F2h	Access	rfu	rfu	rfu
F3h	rfu	rfu	rfu	rfu
F4h	rfu	rfu	rfu	rfu
F5h	Pwd00	Pwd01	Pwd02	Pwd03
F6h	Pwd04	Pwd05	Pwd06	Pwd07
F7h	Pwd10	Pwd11	Pwd12	Pwd13
F8h	Pwd14	Pwd15	Pwd16	Pwd17

3.1.1 芯片唯一序列号(UID)

每一个颗芯片都有一个 7 字节的唯一 UID 码，它和两个校验码共 9 个字节存放在页 00、页 01 和页 02 的第一个字节内。UID 及其校验码是在芯片出厂初始化时写入的，出厂后不可再更改。

根据 ISO14443-3 协议，校验字节 BCC0=CT⊕UID0⊕UID1⊕UID2；BCC1= UID3⊕UID4⊕UID5⊕UID6。其中，UID0 为上海飞聚微电子的厂商代码 53。

3.1.2 OTP 区

03 页为 OTP 区，该页的内容可通过写命令更改，写命令的参数值和 03 页原有的值进行或运算后产生的新值作为 03 页的新值。因此该页上每一位的值只可由写命令置 1，不可置 0。

根据 NFC 论坛官方协议，该页的值已在出厂时进行了初始化，不建议用户更改该扇区内容以完全兼容 NFC 论坛官方协议。该页出厂时的缺省内容请参见下文表格。

3.1.3 LOCK 设置

F8216 共有 5 个只读锁存控制字节，分别为 Lock0,Lock1,Lock2,Lock3,Lock4。这 5 个字节均为 OTP 功能，均可用 Write 命令将任意位置为 1，置为 1 后，该位不可再改写成 0。5 个 Lock 字节的功能如下所述。

静态 LOCK 字节

02 页的 byte2,3 字节的 lock0,lock1 为静态 Lock 字节。这两个字节控制存储器前 16 个页的只读功能设置。各个位的只读锁存功能如下表所示：

	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
LOCK0	L 7	L 6	L 5	L 4	OTP	BL15-10	BL 9-4	BL OTP

	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
LOCK1	L 15	L 14	L 13	L 12	L 11	L 10	L 9	L 8

其中，Lock0 的 Bit3-Bit7,Lock1 的 Bit0-Bit7 分别锁定 04 页至 15 页，这些位的值一旦置为 1 后，相应的页锁定为只读状态，不可再更改其内容。Lock0 的 Bit3 用于锁定 03 页即 OTP 页。Lock0 的 Bit2 用于锁定 15 页至 10 页对应的锁存位，即该位为 1 后，Lock1 的 Bit2 至 Bit7 数值不可再更改。Lock0 的 Bit1 用于锁定 09 页到 04 页对应的锁存位，即该位为 1 后，Lock0 的 Bit4 至 Bit7、Lock1 的 Bit1，Bit0 的数值都不可再更改。Lock0 的 Bit0 用于存定 OTP 页对应的锁存位，即 Lock0 的 Bit3。

动态 LOCK 字节

F0h 页上的前三个字节分别为 Lock2,Lock3，Lock4，这三个字节用于锁定 16 页及以后的页地址，每一位对应的页地址定义如下：

LOCK2	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
	L128-143	L112-127	L96-111	L 80-95	L 64-79	L 48-63	L 32-47	L 16-31

LOCK3	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
	RFU	RFU	L224-239	L208-223	L192-207	L176-191	L160-175	L144-159

LOCK4	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
	RFU	BL208-239	BL176-207	BL144-175	BL112-143	BL80-111	BL48-79	BL16-47

如上表所示，Lock2 的 Bit0-7，Lock3 的 Bit0-4 分别控制 16 个页的只读锁存功能。Lock3 的 Bit5 控制最后两个页的只读锁存功能。Lock4 的 Bit0-Bit6 这 7 个比特实现相应页对应的锁存位的只读锁存功能。比如 Lock4 的 Bit0 置为 1，则 Lock2 的 Bit0,Bit1 将不可再更改。

3.1.4 密钥区

F5h 页到 F8h 页为 128 位 3DES 认证密钥。

在没有认证保护或有认证保护但认证成功的情况下，这四个页的密钥数据可以由 Write 命令或 Compatibility_Write 命令改写。在任何情况下，执行读这四个页数据的命令，如可成功执行，均返回 00h，即任何情况下都不可读出这四个页地址内容。

3.1.5 配置区

F1h 页和 F2h 页为功能配置区，用于定义芯片密钥保护区域及 ASCII 映射等功能。其中包括 Mirror、Rcnt_ascii、Mirror_Page、Auth0、Access 四个配置字节，其存储器位置如下表：

	Byte0	Byte1	Byte2	Byte3
F1h	Mirror	Rcnt_ Ascii	Mirror_ Page	Auth0
F2h	ACCESS	RFU	RFU	RFU

其中：

	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
Mirror	Mirror_Conf		Mirror_Byte		RFU	RFU	Trigger_Mode_L	

	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
Rcnt_ ascii	Trigger_Mode_H		RFU		RFU	Mirror_Conf1		RFU

	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0
Access	PROT	CCFGLCK	RFU	NFC_CNT _EN	NFC_CNT_PW D_PROT	AUTHLIM		

各配置值功能的详细定义如下：

名称	位长	缺省	功能定义
Mirror_Conf	2	00b	定义需要镜像映射的内容，定义如下： 00：无 ASCII 映射 01：对 UID 进行 ASCII 映射 10：对 NFC 计数器进行 ASCII 映射 11：对 UID 和 NFC 计数器进行 ASCII 映射
Mirror_Conf1	2	00b	定义需要镜像映射的内容，定义如下： 00：映射为 Mirror_Conf 定义的内容 01：映射返回为动态签名值 10：映射返回为动态签名值含计数器值 11：Undef
Mirror_Byte	2	00b	定义在 Mirror_Page 页内的 ASCII 映射的起始字节地址。
Trigger_Mode_L	2	00b	00 无触发功能 01 收到第一个 pause 时触发高电平 10 选卡后触发高电平 11 上电触发高电平
Trigger_Mode_H	2	00b	00 定义触发方式为 Trigger_Mode_L 定义的触发方式 01 触发方式为认证成功后触发 10 触发方式为命令触发 11 定义为认证成功后命令触发
Mirror_Page	8	00h	定义 ASCII 映射的起始页地址，大于 03h 时使能 ASCII 映射功能。
AUTH0	8	FFh	定义了认证保护的起始页地址。如果该值定义大于了存储区的有效地址范围，实际上是禁止了芯片的认证功能。
PROT	1	0b	定义了存储空间的保护模式 0：写访问由密钥认证保护 1：读写访问均由密钥认证保护
CFGLCK	1	0b	锁定用户配置区 0：用户配置区打开，可以进行写访问 1：用户配置区关闭，不可改写
NFC_CNT_EN	1	0b	NFC 读计数器使能配置 0：NFC 读计数器关闭 1：NFC 读计数器打开 计数器功能打开后，计数器会在芯片上电后收到第一个读命令或快速读命令后自动加 1。
NFC_CNT_ PWD_PROT	1	0b	NFC 读计数器的密钥保护 0：NFC 读计数无保护 1：NFC 读计数由密钥认证保护 如果认证保护功能打开，读计数值只可在密钥认证后，由 READ_CNT 命令读出计数器值。

AUTHLIM	3	000b	密钥认证失败次数限制 000：认证失败次数无限制 xxx：连续密钥认证失败的最大次数限制 最大值为 7，一旦连续密钥认证失败次数达到这个值，密钥认证将不再成功。

3.1.6 动态签名功能

当 Mirror_Conf1 配置为 01 或 10 后，动态签名值会映射到 Mirror_Page,Mirror_Byte 指定的字节地址。也就是阅读器读到设定地址后，芯片会输出 7 字节 UID＋12 字节的动态签名值的 ASCII 码映射。这个值可用于集成在 NDEF 格式内用于芯片合法性认证。

动态签名值是由芯片内真随机数模块产生一个真随机数明文，再和 UID 一起签名运算，再用芯片内的 128 位密钥加密产生的。它可以做到保证芯片每次上电都有一个变化的加密随机数生成。

3.1.7 存储器出厂配置

16 字节的密钥存储于 F5h,F6h,F7h,F8h 四个页中。可以在认证后，用 WRITE 命令或兼容 Write 命令写入新的密钥值。下图为密钥在存储器中的位置：

用写命令写入密钥值的过程举例如下，key1=0001020304050607h, key2=08090A0B0C0D0E0Fh，则写入的命令为：

A2 F5 07 06 05 04 CRC

A2 F6 03 02 01 00 CRC

A2 F7 0F 0E 0D 0C CRC

A2 F8 0B 0A 09 08 CRC

写入后，密钥区域的值变为如下图所示：

页地址	Byte0	Byte1	Byte2	Byte3
F5h	07	06	05	04
F6h	03	02	01	00
F7h	0F	0E	0D	0C
F8h	0B	0A	09	08

不管配置成什么模式，密钥区域均是不可读的，

3.1.8 存储器出厂配置

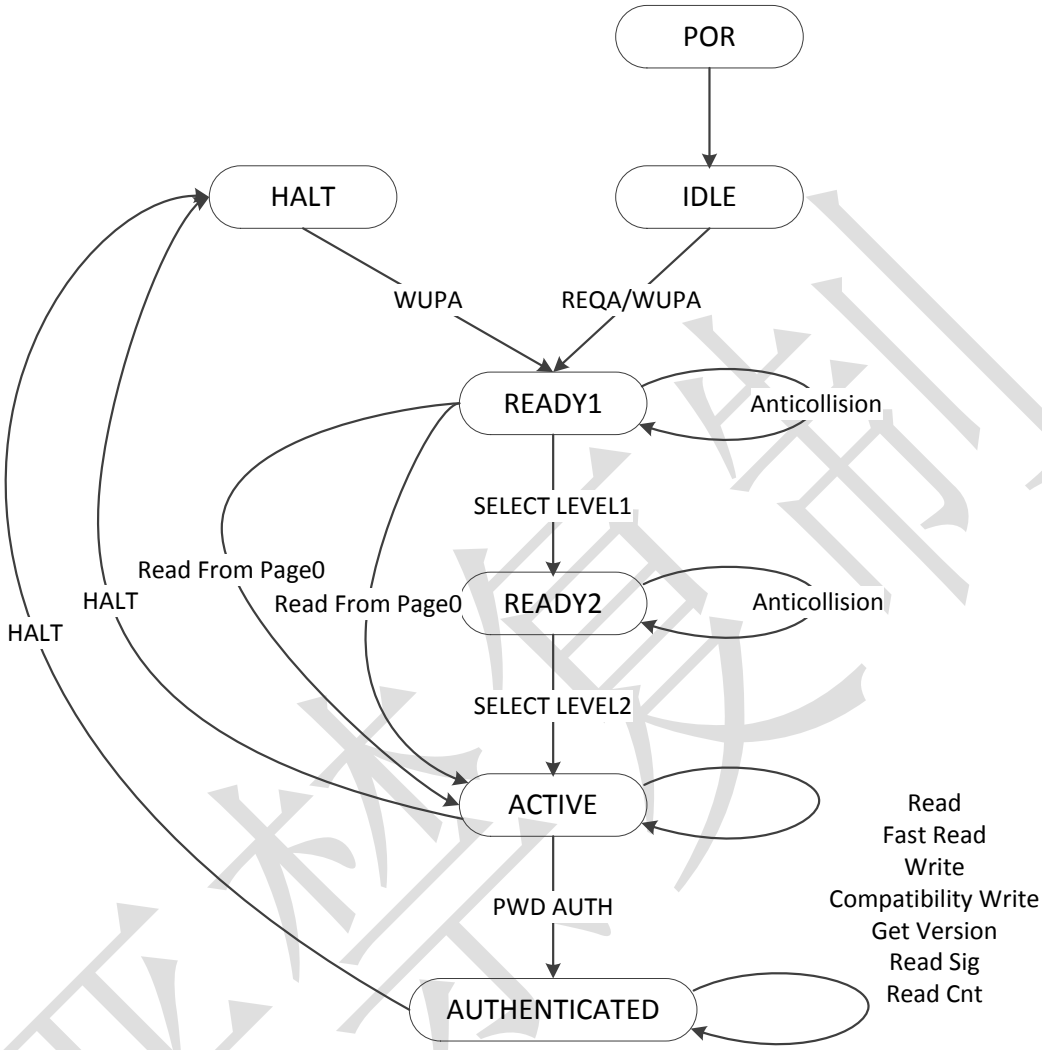
存储器出厂后的默认配置如下表：

地址	Byte0	Byte1	Byte2	Byte3

0	00h	UID0	UID1	UID2	BCC0
1	01h	UID3	UID4	UID5	UID6
2	02h	BCC1	Internal	00h	00h
3	03h	E1h	10h	76h	00h
4	04h	03h	00h	FEh	00h
5	05h	00h	00h	00h	00h
	…	00h	00h	00h	00h
	…	00h	00h	00h	00h
224	EEh	00h	00h	00h	00h
225	EFh	00h	00h	00h	00h
226	F0h	00h	00h	00h	00h
227	F1h	00h	00h	00h	FFh
228	F2h	00h	00h	00h	00h
229	F3h	00h	00h	00h	00h
230	F4h	00h	00h	00h	00h

其中，03 页和 04 页为兼容 NFC 论坛协议的格式化信息，不建议用户改写 03 页的信息，否则会破坏 NFC 官方的协议格式。

3.2 状态图



注：任何状态下，如有任何错误发生，将返回至先前的初始状态，如初始状态为 IDLE，则返回至 IDLE，如初始状态为 HALT，则返回至 HALT 状态。

3.3 指令系统

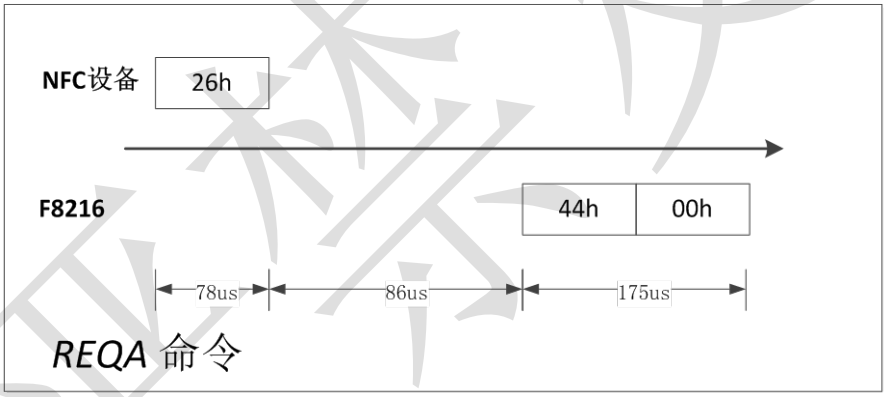
F8216 所支持的指令集表如下：

命令名称	指令代码	说 明
REQA	26h	寻卡指令，场内不在暂停状态的芯片响应
WUPA	52h	唤醒指令，所有场内的芯片响应
Anticollision CL1	93h 20h	第一级防冲突
Select CL1	93h 70h	第一级选卡
Anticollision CL2	95h 20h	第二级防冲突

Select CL2	95h 70h	第二级选卡
HALT	50h 00h	进入暂停状态
Get_Version	60h	读取芯片的版本信息
Read	30h	读数据命令，返回 16 个字节的数据
Fast_Read	3Ah	快速读命令，返回起始页和终止页之间的所有数据
Write	A2h	写数据命令，一次写入 4 个字节
Comp_Write	A0h	兼容写数据命令，一次写入 16 个字节
Read_CNT	39h	返回读计数器的结果
Authenticate Step1	1Ah	第一重 3DES 认证过程，返回 32 位加密随机数
Authenticate Step2	AFh	第二重 3DES 认证过程，返回 32 位加密随机数
Read_SIG	3Ch	返回 32 个字节的 UID 签名数据

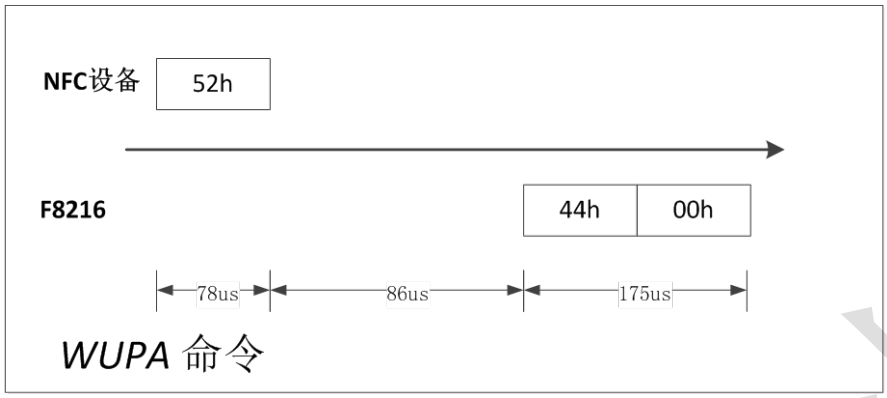
3.3.1 REQA

寻卡指令，根据 ISO14443-3 协议，芯片在 IDLE 状态下可执行该指令，返回 2 个字节的 ATQA。格式如下图：



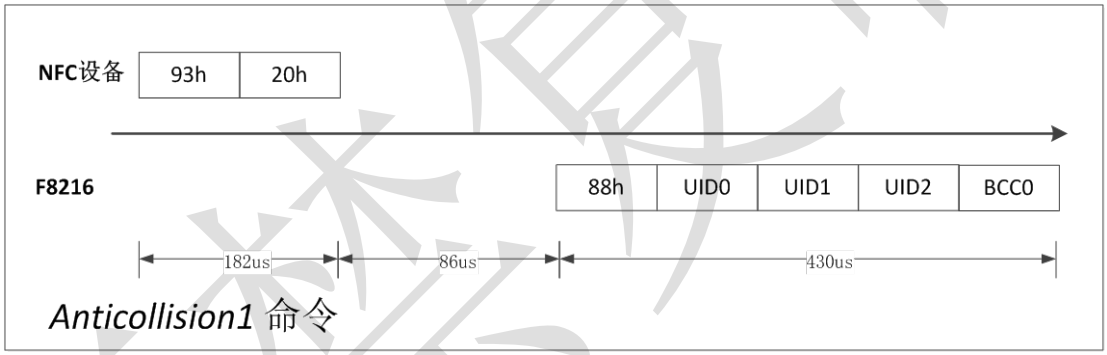
3.3.2 WUPA

唤醒指令，根据 ISO14443-3 协议，芯片在 IDLE 和 HALT 状态下均可执行该指令，返回 2 个字节的 ATQA 信息。格式如下图：



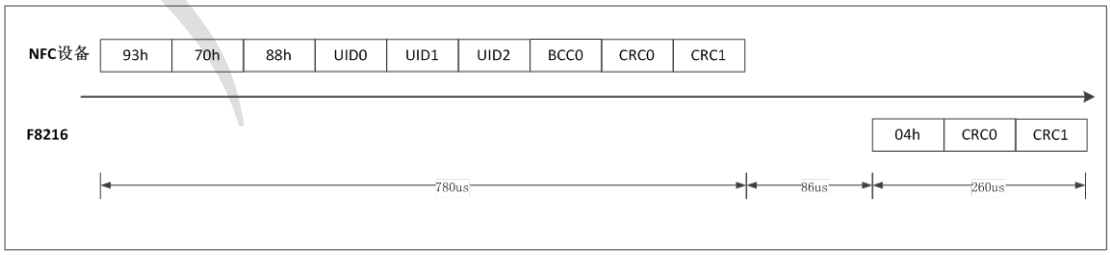
3.3.3 Anticollision CL1

第一级防碰撞指令，命令代码 93，参数为 20 或 nm 及部分 UID，返回为 88h 及前 3 个 UID 字节。该命令在 READY1 状态下有效，命令格式如下 ：



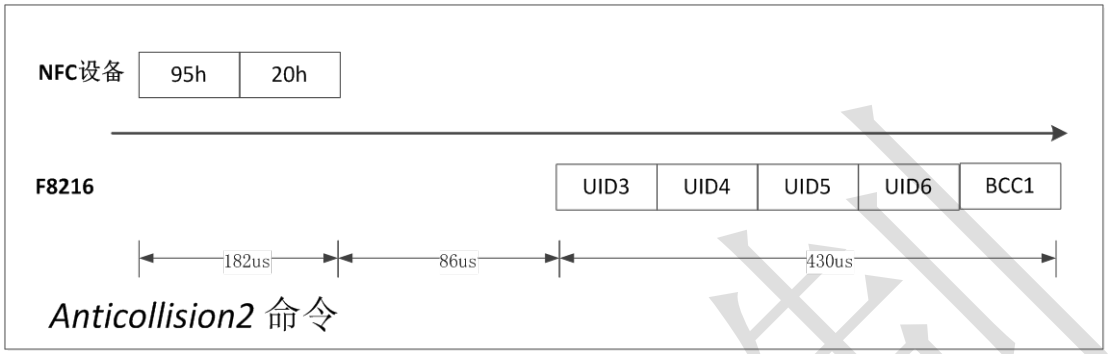
3.3.4 Select CL1

第一级选卡指令，命令代码 93，参数为 70 及 UID 前 3 个字节，返回为 04h。该命令在 READY1 状态下有效，成功后芯片进入 READY2 状态，命令格式如下 ：



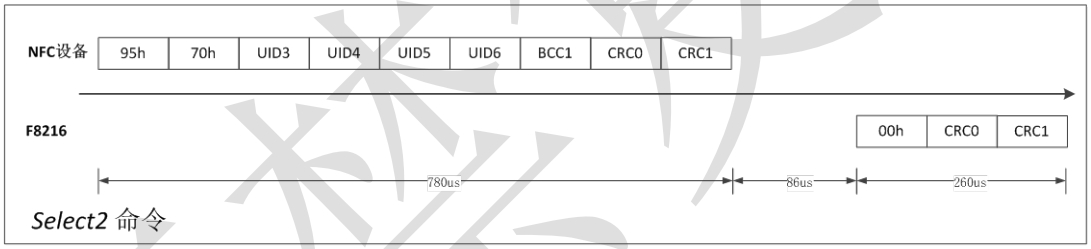
3.3.5 Anticollision CL2

第二级防碰撞指令，命令代码 95，参数为 20 或 nm 及部分 UID，返回为后 4 个 UID 字节。该命令在 READY2 状态下有效，命令格式如下 ：



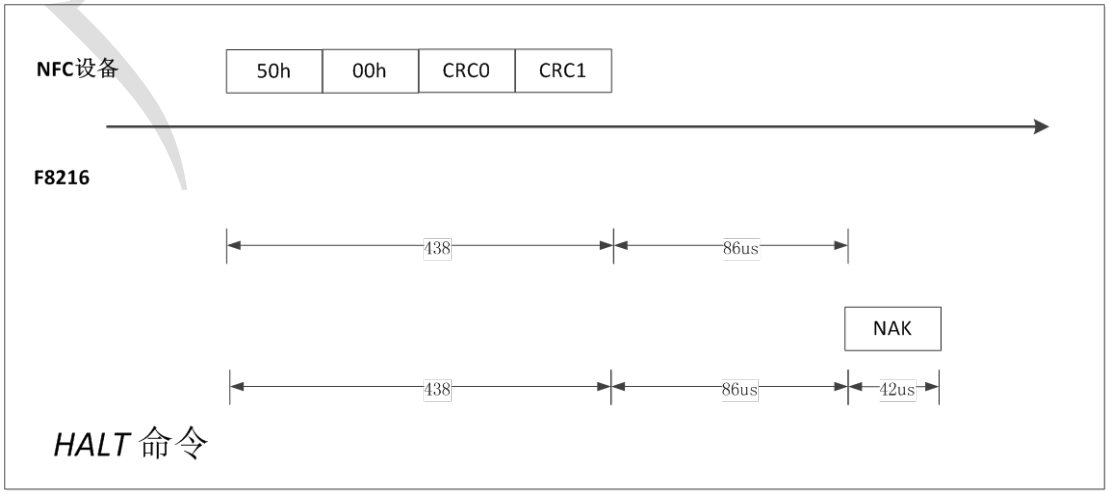
3.3.6 Select CL2

第二级选卡指令，命令代码 95，参数为 70 及 UID 后 4 个字节，返回为 00h。该命令在 READY2 状态下有效，成功后芯片进入 ACTIVE 状态，命令格式如下 ：



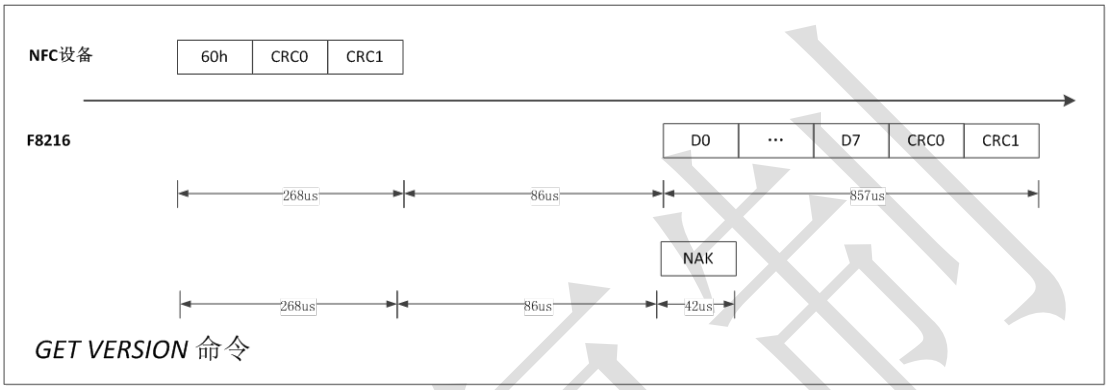
3.3.7 HALT

休眠指令，命令代码 50，参数 00。在 ACTIVE 及 AUTHENTICATED 状态下执行该命令后，芯片进入 HALT 状态，在此状态下，芯片只响应唤醒指令。



3.3.8 Get_Version

获取版本指令。指令代码 60，无参数。该指令返回 D0-D7，共 8 个字节的芯片版本信息。



GET VERSION 命令

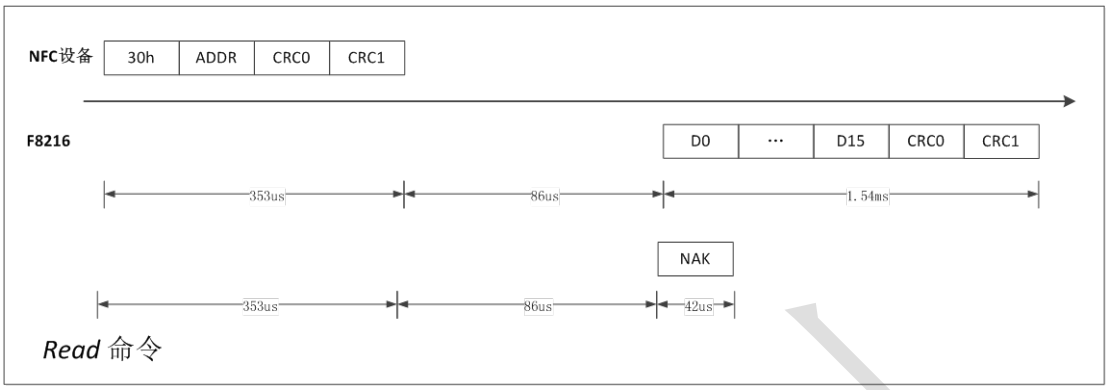
版本信息字节定义如下表：

编号	名称	数值	描述
0	头字节	00h	固定数值
1	厂商代码	53h	上海飞聚微电子厂商代码
2	产品类型	04h	F8xxx 系列产品
3	产品子类型	02h	50pF
4	主版本号	01h	01
5	副版本号	00h	V0
6	存储容量	13h	见下文描述
7	协议类型	03h	ISO/IEC 14443-3 兼容

其中存储容量 13h 的高 7 位等于 9，最低位等于 1，表示芯片容量是介于 2^9 和 2^{9+1} 字节之间的容量，对于 F8216 芯片，用户可用的存储容量为 888 字节。

3.3.9 Read

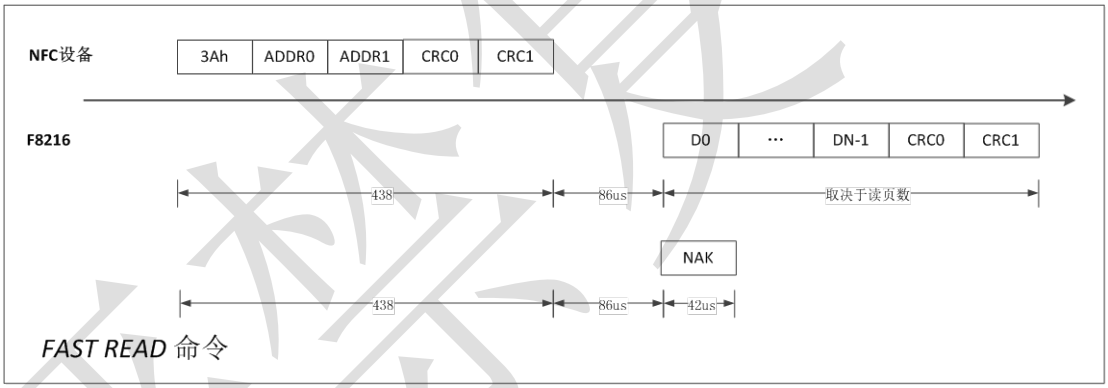
读指令，命令代码 30，一个地址参数。如成功执行该指令返回以地址参数为首页地址的连续 4 页的共 16 个字节的数据。如果连续 4 页地址范围超过了可读取的最大页地址，则从 00 页地址继续读出数据。格式如下：



Read 命令

3.3.10 Fast Read

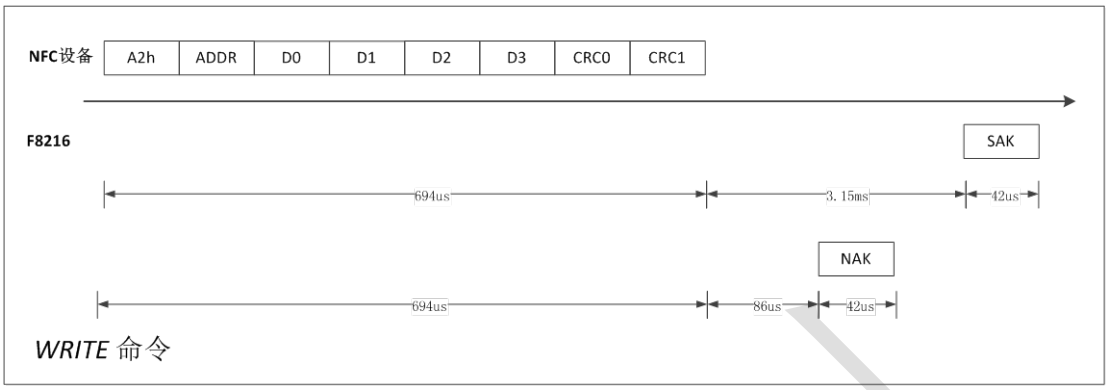
快速读指令，指令代码 3A，两个页地址参数，起始页地址和结束页地址。该指令可返回起始页地址和结束页地址之间定义的所有字节内容，可一条指令读出多于 4 页空间的数据量。指令格式如下：



FAST READ 命令

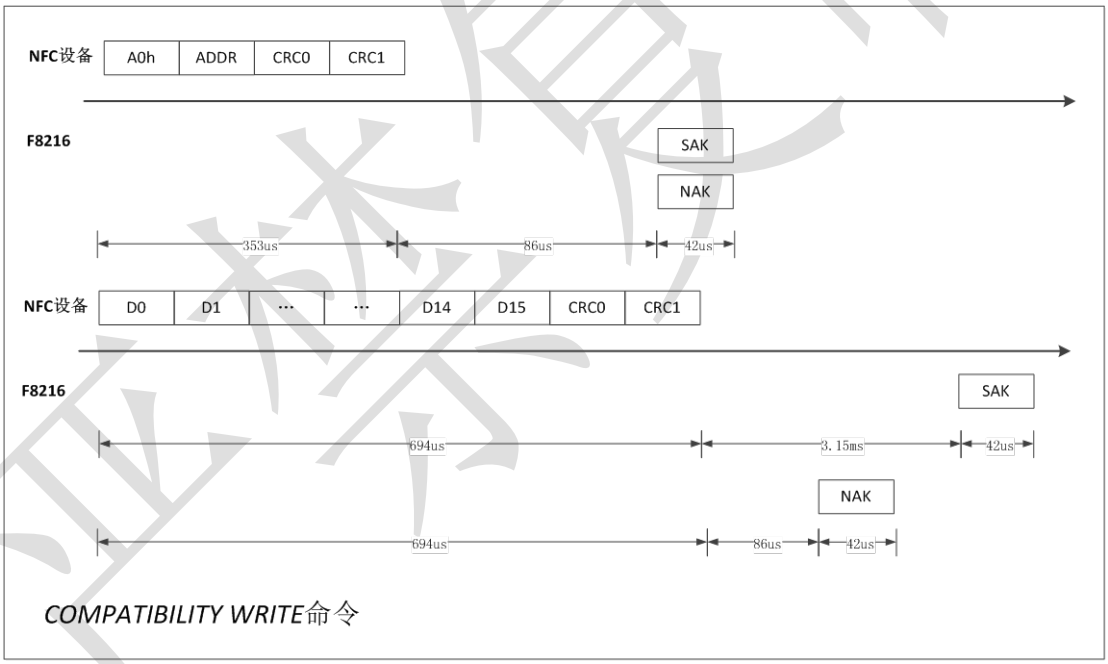
3.3.11 Write

写指令，指令代码 A2，一个字节页地址参数，四个数据字节参数。该指令将四个字节数据写入指令的页地址中。指令格式如下：



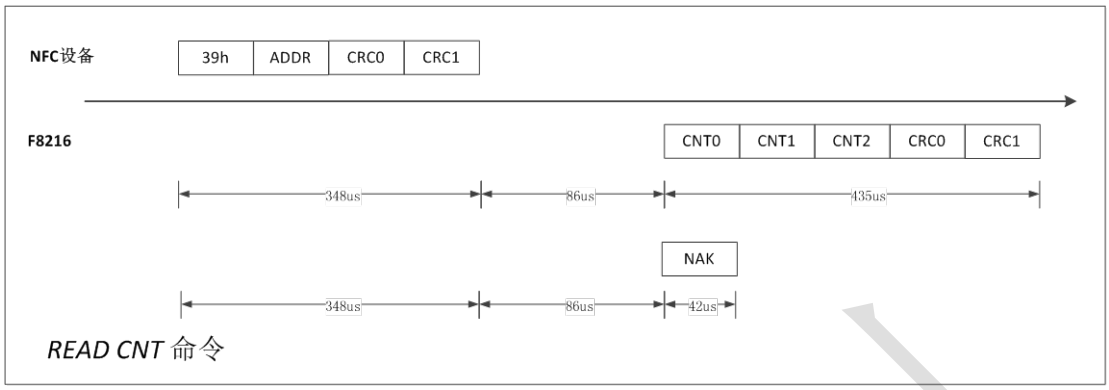
3.3.12 Comp_Write

兼容写指令，指令代码 A0。该指令分两阶段完成，第一阶段传送写地址，第二阶段传送 16 字节数据，但只有前四个字节数据写入该页地址。指令格式如下：



3.3.13 Read_CNT

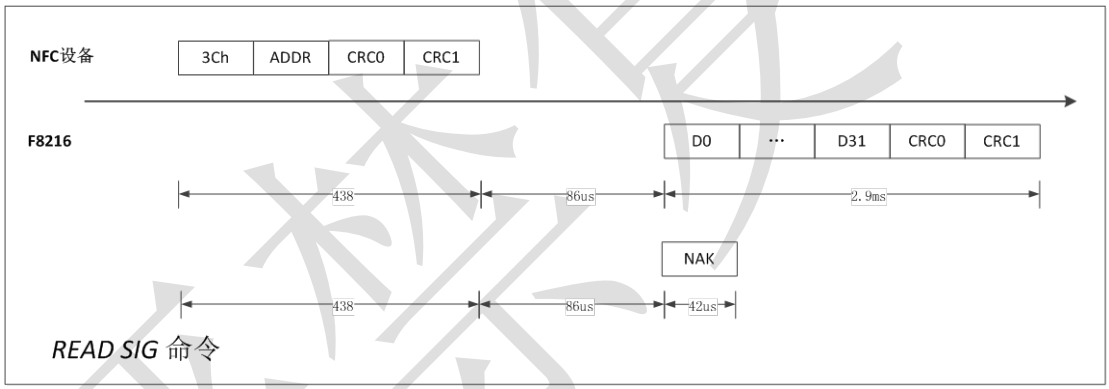
读计数器指令，指令代码 39，参数为计数器地址 02h。该地址可读出 3 字节长的计数器值。计数器的值可由 Read_CNT 指令读出，也可以 ASCII 码映射的方式读出。当配置位 NFC_CNT_PWD_PROT 置 1 后，计数器受到密钥保护，只可在密钥认证通过后由 Read_CNT 指令读出计数器值。该指令格式如下：



READ CNT 命令

3.3.14 Read_SIG

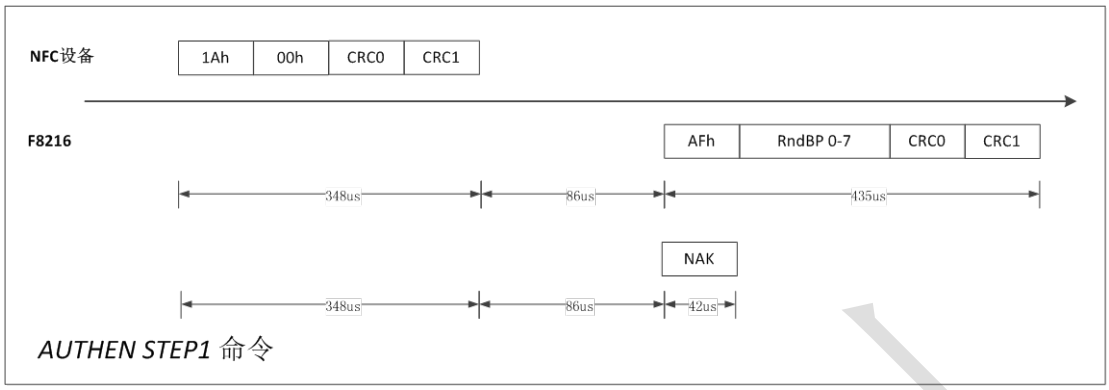
读签名指令，指令代码 3C，参数为一个字节的 00h。该命令返回一个特定的根据芯片 UID 计算出来的 32 字节的 ECC 算法签名值。该签名值用来验证芯片是否属于上海飞聚微电子有限公司。该指令结构如下：



READ SIG 命令

3.3.15 Authen_Step1 命令

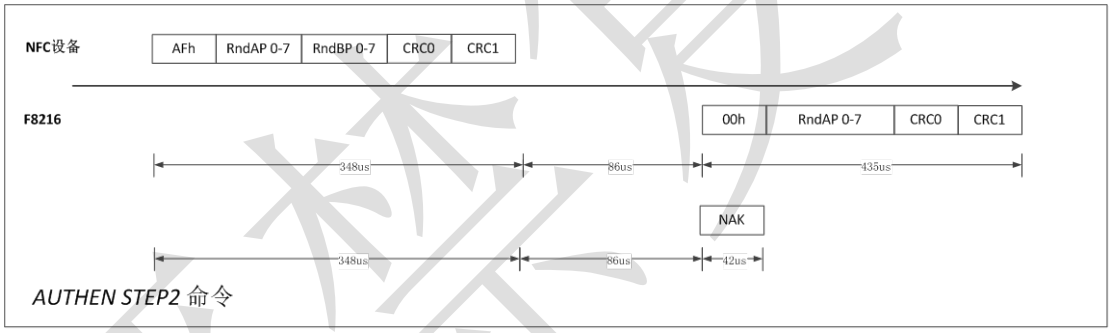
3DES 三重认证的第一步命令，指令代码为 1A，参数为 00。该指令向 F8216 芯片发出认证请求，芯片返回一个 8 字节的加密随机数 RNDBP。该指令结构如下：



AUTHEN STEP1 命令

3.3.16 Authen_Step2 命令

3DES 三重认证的第二步命令，指令代码为 AF，数据为 8 个字节的设备随机数 RNDAP 和 8 个字节的芯片随机数 RNDBP。读写设备收到芯片随机数后解密，变换后重新加密，并发出自己产生的加密随机数和重新加密的芯片随机数。芯片收到后，解密得到原始随机数 RNDA 和 RNDB，并返回一个重新加密的 8 字节的加密随机数 RNDAP，用于设备认证芯片。该指令结构如下：



AUTHEN STEP2 命令

4、电气参数

4.1 极限额定参数

符号	参数	测试条件	范围	单位
Tstg	存储温度范围		-55--- +140	℃
Tj	结温		-55 ---+140	℃
VESD	ESD 电压	-STD-883D	□2	kVpeak
Imax LA-LB	最大输入峰值电流		30	mApeak

4.2 建议工作条件

符号	参数	测试条件	最小值	典型值	最大值	单位
Tjop	工作结温		-25		+85	℃
ILA-LB	输入电流				30	mArms
Fop	工作频率		-	13.56	-	MHz

4.3 性能参数

符号	参数	测试条件	最小值	典型值	最大值	单位
Cres	输入电容	VLA-LB=2Vrms	46	50	54	pF
Tret	EEPROM 数据保持时间	Tamb≤55℃	10			Years
Nwrite	EEPROM 擦写次数		100000			Cycles