电子标签数据存储空间及数据加密说明

一、概述

本文主要对“电子标签数据存储空间及数据加密”两个内容的介绍。

二、目的

主要解答用户在使用 UHF 标签时容易产生的疑惑，加强用户对 UHF 标签的认识。

三、电子标签的数据存储空间

1、IS0/IEC18000-6C 的 Tag 存储空间标准分布图

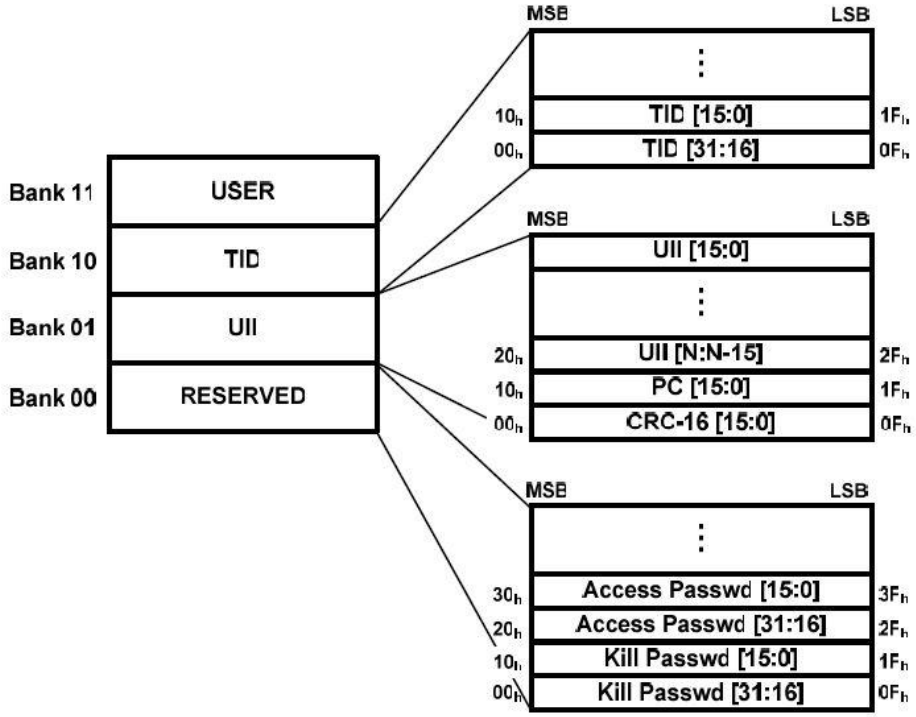

Figure Amd.1-20 — Logical memory map

备注：

- 标准的 UHF 标签是包含这四部分存储区，但是，根据厂商自定义，有的标签没有 USER 区。
- 各个厂商的 Bank01、Bank10、Bank11 存储空间大小也不太一样，具体需参考电子标签的 datasheet

2、标准的电子标签空间分为四个块：

序列	块区（hex）	名称	功能
0	00	RESERVED	存储 access passwords 和 kill passwords
1	01	UII	标签的识别号，用户可以修改
2	02	TID	用户不能修改
3	03	USER	用户操作数据区

2.1 Bank00

RESERVED 区，主要存储 kill passwords 和 access passwords。

2.1.1 kill passwords

kill passwords 存储在保留内存 00h 至 1Fh 的 32 位数值，MSB 优先。默认(未编程)值应为零。询问机应一次性使用标签的 kill passwords 销毁标签，使其保持沉默。如果标签的 kill passwords 为零，则标签不应执行销毁操作。不执行 kill passwords 的标签仍然可以起作用，尽管其零值化的 kill passwords 被永久读锁定和写锁定。

2.1.2 access passwords

access passwords 存储在保留内存 20h 至 3Fh 的 32 位数值，MSB 优先。默认(未编程)值应为零。access passwords 非零的标签应要求询问机在转为保护状态之前发出该口令。不执行 access passwords 的标签仍然可以起作用，尽管其零值化的 access passwords 被永久读锁定和写锁定。

2.2 Bank01

UII 区，包括了 CRC-16 地址从(00_h 到 $0F_h$)，PC 地址(10_h 到 $1F_h$)，和一个 UII 的起始地址，从 20_h 开始的一个区域。它们的起始位为高。

2.2.1 CRC-16

CRC-16 为询问机在保护某个特定的 R=＞T 命令时所使用的和标签在保护某个特定的反向散射 T=＞R 序列时使用的循环冗余码校验。为生成 CRC-16，询问机或标签应首先生成如表 3-1 所示的 CRC-16 先驱，然后取生成的先驱的二进制反码形成 CRC-16。

CRC-16 保护的序列为标签在盘存操作期间反向散射的 PC 位和 EPC。由于询问机可以发出将全部或部分 CRC-16 包括在 mask 中的 Select 命令，并可以发出 Read 命令以便使标签反向散射 CRC-16，因此 CRC-16 从逻辑上映射到 EPC 存储器中。上电后，标签应计算 EPC 存储位置 10h 上的 CRC-16，直至 EPC 的末端(不一定直至 EPC 存储器的末端，但必须直至 PC 中 length field 规定的 EPC 的末端)，并将所计算的 CRC-16 映射到 EPC 存储器 00h 至 0Fh 中，MSB 优先。由于{PC+EPC}存储在 EPC 存储器词界上，因此应在词界计算该 CRC-16。

为便于信息检验，询问机或标签可以将 CRC-16 添加到所传输的信息上，并重新计算 CRC-16。若该信息仍然可靠，则其余项将是 1D0Fh。

表 3-1-CRC-16 先驱

CRC-16 先驱				
CRC 型	长度	多项式	预置	余项
ISO/IEC 13239	16 位	X16+X12+X5+1	FFFFh	1D0Fh

2.2.2 协议-控制(PC)位

PC 位包含标签在盘存操作期间以其 EPC 反向散射的物理层信息。EPC 存储器 10h 至 1Fh 存储地址存储有 16PC 位，PC 位值定义如下：

- 10_h—14_h 位：标签反向散射的(PC+EPC)的长度，所有字为：
  00000_2：一个字(EPC 存储器 10_h—$1F_h$ 存储地址)
  00001_2：两个字(EPC 存储器 10_h—$2F_h$ 存储地址)
  00010_2：三个字(EPC 存储器 10_h—$3F_h$ 存储地址)
  ……
  11111_2：32 个字(EPC 存储器 10_h—$1FF_h$ 存储地址)
- 15_h—16_h 位这不同的标准里面有不一样的定义：
  - 15_h—16_h 位：RFU(ISO-18000-6C 里定义为 00_2)
  - 15_h—16 h 位：在“EPC_C1G2_V1.20”中有明确的定义

Bit15：作为 USER 区的指示（UMI）。如果 Bit15 没有被置位，标明标签没有使用 USER 区或者 USER 区没有包含数据信息。如果 Bit15 被置位，则 USER 区包含信息。一张标签可以通过以下两种方式来执行 UMI，除非标签被块锁。

方法 1：标签计算 UMI。在上电时，在计算标签的 StoredCRC 之前,标签将计算 USER 区的 bit3 到 bit7 逻辑或之后的值映射到 UII 区的 bit15，标签将计算 UMI 后的值再计算出 StoredCRC。如果读写器修改了 USER 区的 bit3 到 bit7 位，标签将重新计算并重新映射 UII 区的 bit15。这个 UMI 不可直接写入，当读写器写 StoredPC 值时，标签将忽略 bit15 位。

方法 2：读写器写 UMI，如果读写器在 USER 区的 bit3 到 bit7 位写 0 值，则 UII 区的 bit15 位将清除。如果为非 0 值，则 bit15 位置位。如果读写器给标签的 EPC 区 lock 或者 permalock，依次地，也对 USER 的从 00 开始的一个字 lock 或者 permalock，反之亦然。后者要求 USER 区包含数据，但是擦出将不会引起指示错误，反之亦然。

Bit16：一个 XPC_W1 指示（X1）。如果 bit16 没有被置位，标明标签没有执行 XPC_W1 或者 XPC_W1 值为 0，这个种情况下，标签在 ACK 回应时将返向散射它的 StoredPC 或者 PacketPC,但是没有 XPC_W1。如果 bit16 置位，标签将执 XPC_W1 里的 1 位或者更多位为非 0。后者标签在 Inberntory 轮询时将立即返向散射 StoredPC 或者 PacketPC。

如果一张标签在上电时在计算 StoredCRC 之前执行 XPC_W1，标签将按位逻辑或计算它的 XPC_W1 并且映射计算的值到 bit16（例如：写入 X1）。标签将使用这个被计算的 X1 值计算它的 StoredCRC。如果读写器重新委托标签，然而标签将重新计算并重新映射它的 X1 值到 bit16。在重新计算 X1 之后，这个 StoredCRC 可能不正确直到读写器周期性给标签供电。X1 位不能被读写器直接写，当读写器写标签的 StoredPC 时，标签将忽略这个数据值给 bit16。

- 17_h—$1F_h$ 位：默认值为 00000000_2 且可以包括如 ISO/IEC 15961 定义的 AFI 在内的计数系统识别(NSI)。NSI 的 MSB 存储在 18_h 的存储位置。

默认(未编程)PC 值应为 0000h。

截断应答期间，标签用 PC 位代替 00000_2。

若询问机在存储器写入期间修改 EPC 长度，并希望标签继续反向散射所修改的 EPC，那么询问机必须要将新(PC+EPC)或修改后的(PC+EPC)写入标签 PC 的前五位。若询问机试图将不被该标签支持的(PC+EPC)长度写入该标签 PC 的头五位，则标签应反向散射错误代码。

上电时，标签应通过 PC 前五位指定的(PC+EPC)字数而不是整个 EPC 存储器长度计算 CRC-16。

2.2.3 EPC

EPC 为识别标签对象的电子产品码。EPC 存储在以 20h 存储地址开始的 EPC 存储器内，MSB 优先。询问机可以发出选择命令，包括全部或部分规范的 EPC。询问机可以发出 ACK 命令，使标签反向散射其 PC、 EPC 和 CRC-16(在特定情况下该标签可以截断应答。最后，询问机可以发出 Read 命令，读取整个或部分 EPC。

2.2.4 UII 格式

本文档中所谓的 UII 包含 PC bits。UII 的前两个字节是 PC（Protocol-control）位，其格式见表 3-2。

表 3-2 PC bits 格式

Bits 0 ~ 4	Bits 5 ~ 6	Bits 7 ~ 15
以 word（两个字节）为单位的 PC 和 UII 的总体长度	未定义	NSI（未使用）

注：UII 从低位开始传输。

PC 的前五位表示 PC 和 UII 的总体长度。例如，

PC bits 0~4（bin）	PC+UII 长度（字节）
00000	2
00001	4
00010	6
…	…

整段 UII 的数据信息是由 PC 加上 EPC 构成。所以，用户可以通过 PC 的前 5 位计算出整个 UII 的长度。公式： LengthUII = (((UII[0] >> 3) & 0x1F) + 1) * 2

单位： 字

节。例如：

一张标签的 UII(hex) = 30 00 12 34 56 78 53 40 00 00 12 34 85

1A UII[0] = 0x30;

根据公式：LengthUII = (((UII[0] >> 3) & 0x1F) + 1) * 2

计算结果：LengthUII = 14

所以整段卡号的长度就为 14 个字节。

如果您想写一张标签的 UII 总长度为 12 个字节根据公

式：LengthUII = (((UII[0] >> 3) & 0x1F) + 1) * 2 = 12 计算

结果：UII[0] = 0x28

所以将 UII[0] =0x28 写入 UII 的第一个字节之后的卡号为：28 00 12 34 56 78 53 40 00 00 12 34

综上所述，实际计算长度为 UII[0]的前 5 个比特，具体细节请参考 ISO18000-6-C 协议。

2.3 Bank02

TID 存储区从 00h 至 07h 的包含了 ISO/IEC15963 类别识别项值 E0 或者 E2 之一。TID 存储区从 07h 以上的存储单元的定义注册管理部门将根据为类别识别定义。最少，将包含询问器充足的辨认信息。TID 也许标记了厂商的细节数据。

2.4 Bank03

USER 存储区，提供给用户存储自己的数据内容。

四、数据加密

对于 UHF 标签的数据加密可以使用“LOCK 命令”给数据加锁，防止数据被非法操作。

注意：在使用“LOCK 命令”的时候，关于 Lock-Command Payload 的说明如下，具体详情请参考“ISO/IEC18000-6C 协议”。

Lock-Command Payload 是二十位的数据，高十位是 Mask，低十位是 Action。其格式见表 4-1。当 Mask 置为 1 时对应的 Action 位有效。Action 位的含义见表 4-2。

表 4-1 Lock-Command Payload 数据格式

Kill password		**Access password**		**UII memory**		**TID memory**		**User memory**	
19	18	17	16	15	14	13	12	11	10
Skip/ Write	Skip/ Write	Skip/ Write	Skip/ Write	Skip/ Write	Skip/ Write	Skip/ Write	Skip/ Write	Skip/ Write	Skip/ Write
9	8	7	6	5	4	3	2	1	0
Pwd read/ write	Perma lock	Pwd read/ write	Perma lock	Pwd write	Perma lock	Pwd write	Perma lock	Pwd write	Perma lock

表 4-2 Lock Action 位

Pwd-write	**Permalock**	**描述**
0	0	相应数据段在 OPEN 或 SECURED 状态下可写入
0	1	相应数据段在 OPEN 或 SECURED 状态下永久可写入，相应数据段不可锁定
1	0	相应数据段在 SECURED 状态下可写入，OPEN 状态下不可写入
1	1	相应数据段在任何状态下不可写入
Pwd-read/write	**Permalock**	**描述**
0	0	相应数据段在 OPEN 或 SECURED 状态下可读取和写入
0	1	相应数据段在 OPEN 或 SECURED 状态下永久可读取和写入，相应数据段不可锁定
1	0	相应数据段在 SECURED 状态下可读取和写入，OPEN 状态下不可读取和写入
1	1	相应数据段在任何状态下不可读取和写入

备注：注意 Action 中的定义，有的数据块被锁住后防止写操作，有的既防止写操作也防止读操作。通过 Lock 之后的数据块在没有正确的 access passwords 是不能进行相关操作的。

ACCESS 操作

数据经加密后，欲对加密的数据操作，必须通过在 ACCESS 下的访问，使用正确的 access passwords。

access passwords 存储在保留内存 20h 至 3Fh 的 32 位数值，MSB 优先。默认(未编程)值应为零。access passwords 非零的标签应要求询问机在转为保护状态之前发出该口令。不执行 access passwords 的标签仍然可以起作用，即使其零值化的 access passwords 被永久读锁定和写锁定。