Advanced Card Systems Ltd.
Card & Reader Technologies

ACOS-LITE

功能规格书 V1.01

info@acs.com.hk
www.acs.com.hk

目录

图目录

1.0. 简介

本文件详细介绍了龙杰智能卡有限公司（Advanced Card Systems Ltd., ACS）自主研发的 ACOS-LITE 卡的特性和功能。

1.1. 特性

ACOS-LITE 具有以下特性：

- 连续的 8 K 字节 EEPROM 应用数据存储容量
- 符合 ISO 7816 第 1、2、3 部分；支持 T=0 直接模式协议
- 可实现高速传输（9.6 Kbps - 223.2 Kbps）
- 功能与存储卡兼容
- 设置四组密码
- 支持 3DES 密码加密提交
- 密码可由持卡人更新

1.2. 技术规格

以下是 ACS-LITE 卡的技术参数。

1.2.1. 电气参数

- 工作电压：5V DC +/-10%（A 类）与 3V DC +/-10%（B 类）
- 最大电源电流：< 10 mA
- ESD 保护：≤ 4 KV

1.2.2. EEPROM

- 容量：8 KB
- EEPROM 耐久性：1 万次擦写
- 数据存储记忆：10 年

1.2.3. 环境温度

- 工作温度：-25 °C - 85 °C
- 存储温度：-40 °C - 100 °C

2.0. 复位和复位应答

硬件复位（例如：上电）后，卡片会按照 ISO 7816 第 3 部分的规定传送复位应答（ATR）信号。ACOS-LITE 支持 T=0 的协议类型，但尚未实现协议类型选择功能。

卡片通信中各个位的编码采用正向约定，也就是说，逻辑电平“1”对应的是 I/O 的 Z 状态。

通过历史字节发送的 14 字节数据将在下面介绍。

下面是 ATR 传送的数据：

TS	T0	TA1	TB1	TD1	14 个历史字节
3Bh	BEh	95h	00h	00h	-

通过历史字节发送的 14 个字节的字符串组成如下：

T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14
41h	00h	00h	配置块　字节 8 - 15								00h	90h	00h

3.0. EEPROM 结构

EEPROM 的结构如下：

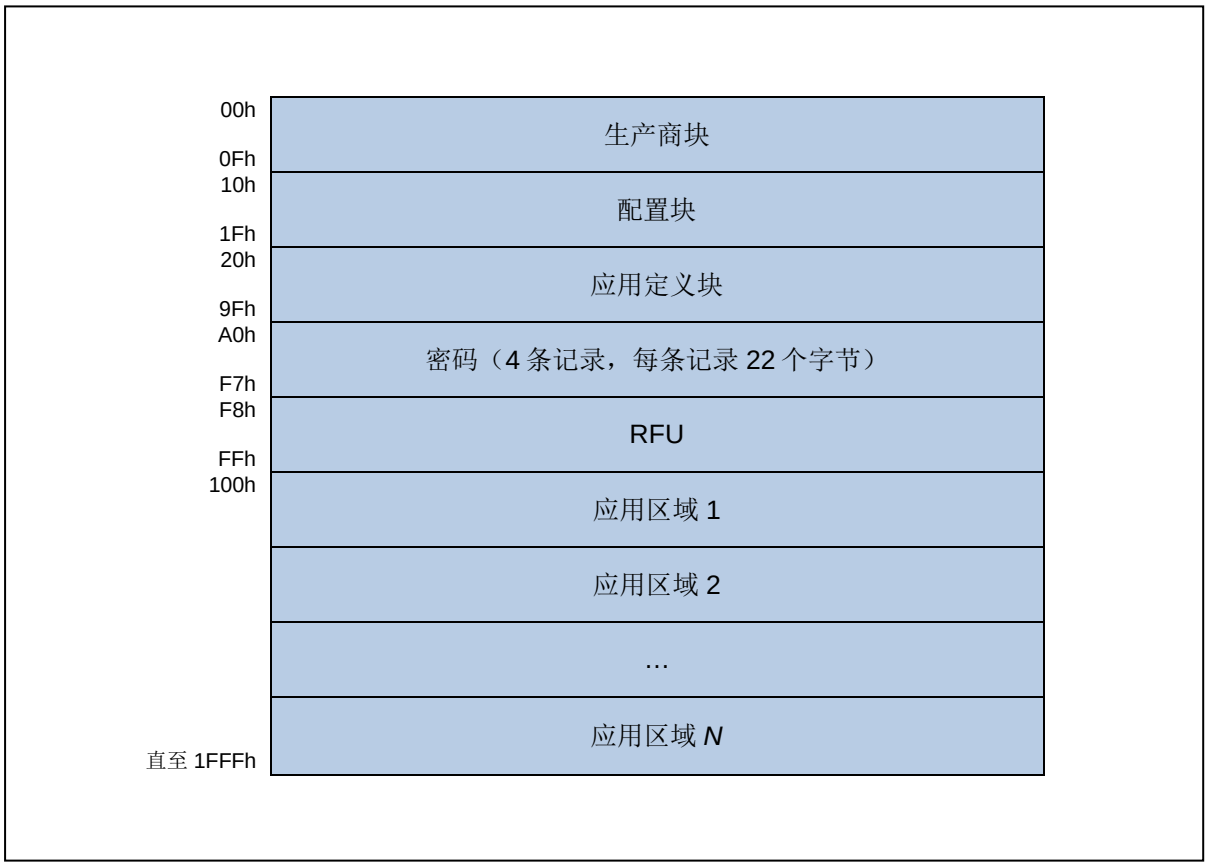

图1 ：EEPROM 内存图

下面将讨论各个块的具体内容。

3.1. 生产商块

生产商块由 ACS 控制，内容不可写。

工程样品默认为将发行商标识符置为 00h..00h。但对于大宗的 ACOS-LITE 卡订单，ACS 会为每位合作伙伴分配发行商标识符。用户可以自由读取生产商块，但不允许对其进行写访问。

3.2. 配置块

配置块用于定义多个卡片选项。用户可以自由读取该块，但进行写入操作时需要验证 SC0。

3.3. 应用定义块

应用定义块允许为各个数据区域或**单向计数器**区域定义不同的访问条件。存储空间从 0100h 开始延伸至 1FFFh。

用户可以自由读取应用定义块，但对该块进行写操作时需要验证 SC0。

3.4. 应用密码

卡片提供了四组应用密码 – SC 0..3，并在几个长度为 22 字节的应用密码记录中对其进行描述。

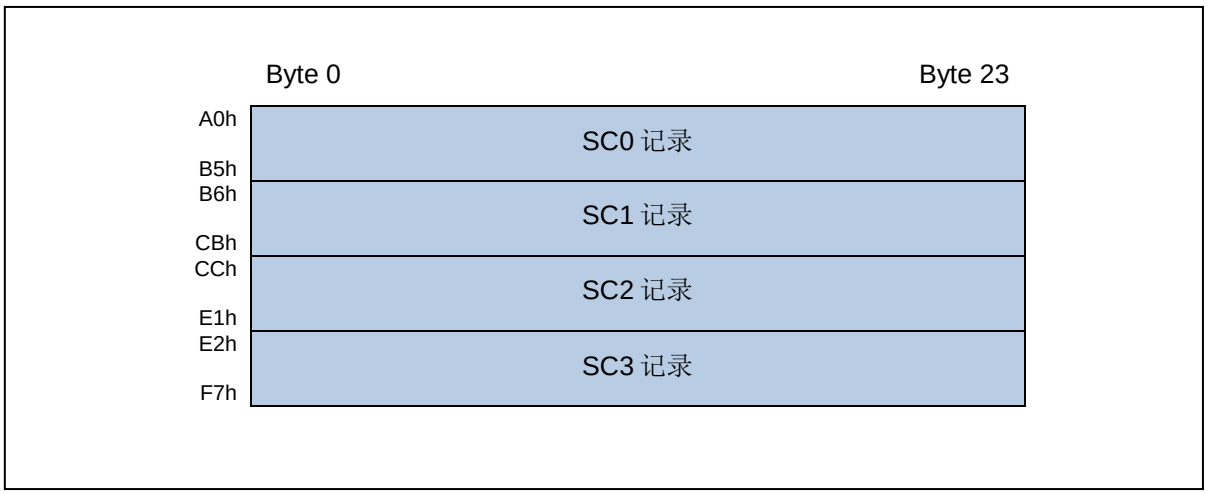

图2 ：密码

默认密码是第一组应用密码。对配置块、应用块和此密码块进行写入操作前需要提交密码 SC0。如果在应用密码相应的 Type 数据域禁止了读取访问，则绝不允许读取该应用密码，并总是返回零。

4.0. 安全

4.1. 内存保护位（MPB）

内存保护位（MPB）用于保护对二进制内存数据和 OWC 数据的更新访问。就如一些存储卡一样，卡片的每个字节都能受到保护，从而可以不按照 UPDATE MEMORY 命令进行更新。对于不同类型的内存来说，MPB 的功能各有不同。区域只能由“不受保护”设置为“受保护”，并且不能够重置。但 MPB 可以自由读取。

4.2. 密码

密码可以以明文或者密文的方式进行提交或修改，此节将对各种情形进行介绍。

4.2.1. 密码提交

密码提交通过普通的 APDU 命令来完成。对于将要接受此类密码提交的 ACOS-LITE 卡，一定不要设置密码 SCx 在 TYPE 数据域的 b7 位。

4.2.2. 密码加密提交

如果设置了 SCx 在 TYPE 数字域的 b7 位，则密码可以经过加密后提交给 ACOS-LITE 卡。应用程序开发人员首先要读取一个由卡片产生的 8 个字节的随机数，然后将其用作 3DES 操作的数据输入，从而完成密码加密提交。3DES 操作的密钥是长度为 16 个字节的 SC 值。

4.2.3. 密码更新

用户可以通过校验原始 SCx 来实现密码更新。要启用密码更新，相应 SCx 的 TYPE 数据域中的 b6 位必须设置为 0。对于要接受明文密码更新的 ACOS-LITE 卡，一定不要设置密码 SCx 在 TYPE 数据域的 b7 位。

4.2.4. 密码加密更新

密码也可以通过加密的 CHANGE SECRET CODE 命令进行更新。对于加密的密码 SCx，一定要设置其在 TYPE 数据域的 b7 位。

5.0. 生命支持应用

这些产品的设计并非用于生命支持设备或系统，在这些设备或系统中对这些产品的误操作可能导致人身伤害。如果 ACS 客户将这些产品使用于或者销售用于此类应用，则他们应该自行承担相应的风险，而且同意赔偿由于不当使用或销售从而给 ACS 造成的损失。

6.0. 联系信息

如需了解其他信息，请访问 ACS 网站 http://www.acs.com.hk。

如需销售咨询请发送邮件至 info@acs.com.hk。