

电子钱包读写实验

一、实验编号及名称

编号：IES_IS014443_04

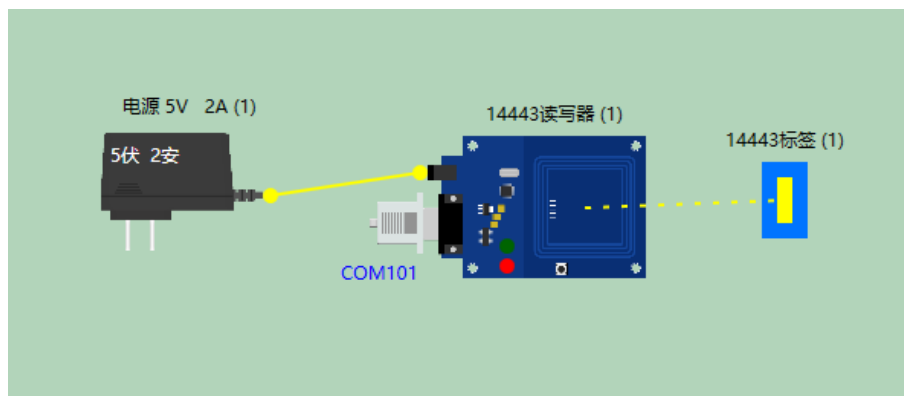
名称：电子钱包读写实验

二、实验目的

- 1、掌握电子钱包的工作流程和原理思路；
- 2、初步了解每个块的权限值的概念；
- 3、掌握初始化电子钱包的详细步骤和规律。

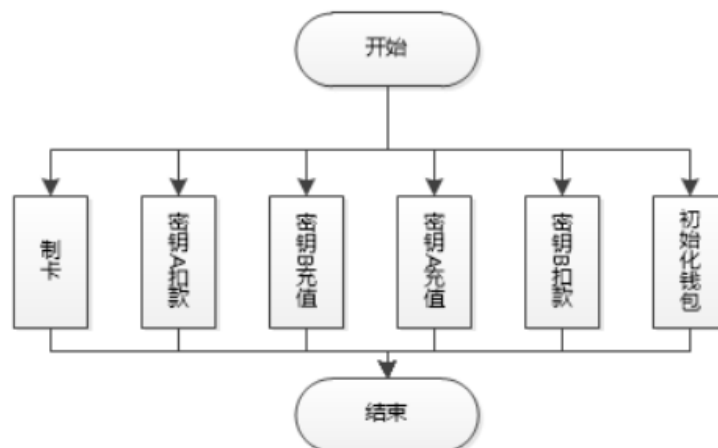
三、实验设备

IS014443 读写器、串口线、5V，2A 电源、IS014443 卡片。在《物联网虚拟仿真实验平台》中按照下图所示进行设备的连接和串口的配置。



注：上图中 COM101 为读写器设备通过串口线与上位机连接的串口号

四、实验内容说明



如上图所示，本实验分为五项内容，包括制卡、密钥 A 扣款、密钥 B 充值、密钥 A 充值、密钥 B 扣款、初始化钱包。本实验的目的是为让学生掌握电子钱包的操作流程和说明以及初始化电子钱包的规律和原理。

五、实验操作

1、制卡



点击红框中的制卡后，出现制卡界面。

点击【打开】按钮，打开串口。然后点击【制卡】完成制卡实验。

注：打开串口成功后，在进行操作时，请保证你要操作的卡必须是一张空白卡，没有对这张卡进行过密钥修改和权限更改等相关操作，否则后续的操作是无法进行。

注：如果用了使用过的卡片，更换卡片之后只需重新点击打开串口，系统会自动读取新卡片标签并显示到界面。

说明：本实验是对扇区 2，块 0 块地址为 8。点击制卡时进行设置电子钱包、密钥修改、权限修改。将块地址为 8 的区块设置为电子钱包，并且充值 100 元，然后修改该扇区的 A 密钥为 AAAAAAAAAAAAAA，B 密钥修改为 BBBBBBBBBBBBBB，控制权限修改为“08778F69”。

2、密钥 A 扣款

(1) 寻卡



点击【寻卡】按钮，自动获取卡片。

(2) 选卡



点击【选卡】，选择你读取到卡号的卡片。

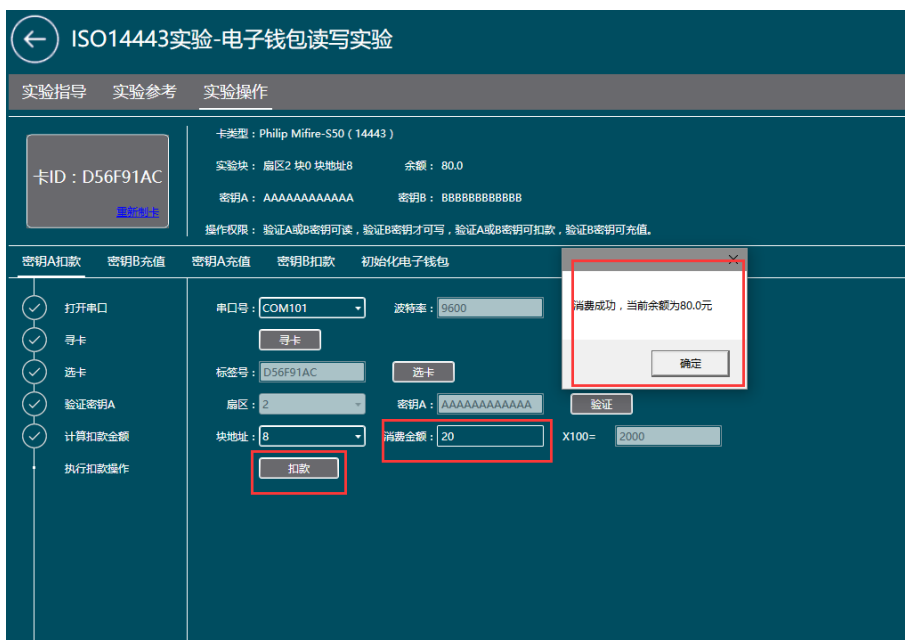
(3) 验证



点击【验证】，验证 2 扇区的 A 密钥，如果提示验证成功，就可对这个扇区进行读取操作，否则无法进行读取操作。

注：如果在验证时，发现你所填密钥与制卡时的密钥是一样的，但仍然提示失败，原因可能是：可能场区内没有读取到该卡、可能是场区内读到另外一张卡。

(4) 扣款



输入消费金额，点击【扣款】按钮，成功消费，提示当前余额。

注：在消费金额中，输入数字，如果输入其他非数字的话会自动清空，将输入的金额数乘以 100 得到要扣款的金额数，乘以 100 的原因是高

频 14443 卡片的数据块作为电子钱包时，不支持存储小数，只支持整数的加减。所以在本实验中进行了数据处理。

3、密钥 B 充值

(1) 寻卡



打开串口，点击【寻卡】按钮。

(2) 选卡



选择你读取到卡号的卡片，点击【选卡】按钮。

(3) 验证



验证 2 扇区的 B 密钥，如果提示验证成功，就可对这个扇区进行写入操作，否则无法进行读取操作。

(4) 填写数据



输入充值金额，点击充值金额。提示充值成功，显示当前余额。

4、密钥 A 充值

(1) 寻卡



打开串口，点击【寻卡】按钮。

(2) 选卡



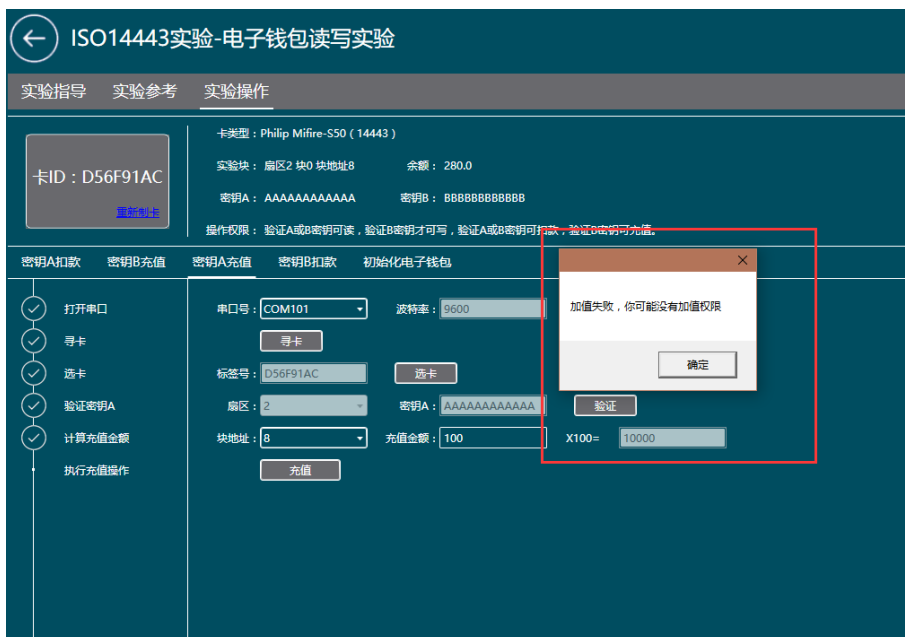
选择你读取到卡号的卡片，点击【选卡】按钮。

(3) 验证



点击【验证】按钮，提示密钥 A 验证成功。

(4) 充值



输入充值金额，点击【充值】按钮，提示充值失败。

注：当时在验证 A 密钥充值时，提示失败，并没有权限进行验证密钥 A 充值，因为在制卡时已经将权限修改为验证 A 密钥可扣款不可充值，验证 B 密钥可扣款可充值。

5、密钥 B 扣款

(1) 寻卡



打开串口，点击【寻卡】按钮。

(2) 选卡



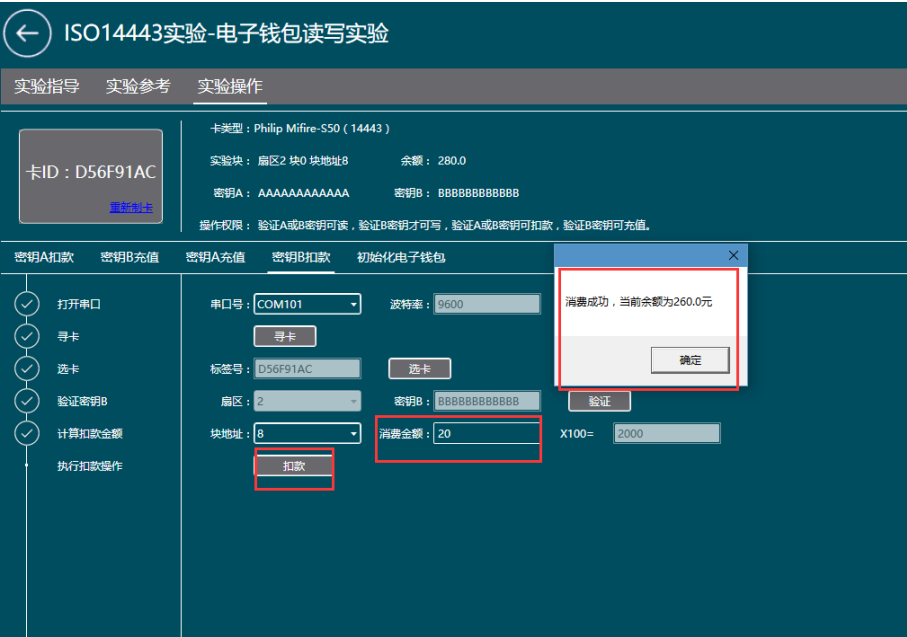
选择你读取到卡号的卡片，点击【选卡】按钮。

(3) 验证



点击【验证】按钮，提示密钥 B 验证成功。

(4) 读取数据



输入消费金额，点击【扣款】按钮，提示消费成功，并显示当前余额。

6、初始化电子钱包

(1) 寻卡



打开串口，点击【寻卡】按钮。

(2) 选卡



选择你读取到卡号的卡片，点击【选卡】按钮。

(3) 验证



点击【验证】按钮，提示密钥 B 验证成功

(4) 转十六进制



输入初始金额，点击【转十六进制】按钮。将要初始化电子钱包的块区的块地址转化为十六进制，以及初始金额的数值转化为十六进制。

(5) 取反

←

ISO14443实验-电子钱包读写实验

实验指导

实验参考

实验操作

卡ID：D56F91AC

重新制卡

卡类型：Philip Mifire-S50 (14443)

实验块：扇区2 块0 块地址8 余额：260.0

密钥A：AAAAAAAAAAAA 密钥B：BBBBBBBBBBBB

操作权限：验证A或B密钥可读，验证B密钥才可写，验证A或B密钥可扣款，验证B密钥可充值。

密钥A扣款

密钥B充值

密钥A充值

密钥B扣款

初始化电子钱包

计算初始字符串

电子钱包块结构实际上与普通块一样，只不过是按照指定的格式组织后，系统便认为他是电子钱包，能按照电子钱包执行增减值操作。

电子钱包块的存储仅支持整数，所以需要数据进行处理，存储金额时，可以将数值乘以100，以下是电子钱包格式表，以金额100为例（实际上写入的是10000）：

| 金额正 | 金额反 | 金额正 | 区块正 | 区块反 | 区块正 | 区块反 |
|-------------|-------------|-------------|-----|-----|-----|-----|
| 10 27 00 00 | EF D8 FF FF | 10 27 00 00 | 09 | F6 | 09 | F6 |

块地址：0

初始金额：100

X100=

10000

转十六进制

块地址：09

初始金额：10270000

取反

块地址反：F6

金额反：EFD8FFFF

计算写入值

点击【取反】按钮，块地址转化为十六进制后，在进行取反。同时十六进制的初始金额值也进行取反。

（6） 计算写入值

←

ISO14443实验-电子钱包读写实验

实验指导

实验参考

实验操作

卡ID：D56F91AC

重新制卡

卡类型：Philip Mifire-S50 (14443)

实验块：扇区2 块0 块地址8 余额：260.0

密钥A：AAAAAAAAAAAA 密钥B：BBBBBBBBBBBB

操作权限：验证A或B密钥可读，验证B密钥才可写，验证A或B密钥可扣款，验证B密钥可充值。

密钥A扣款

密钥B充值

密钥A充值

密钥B扣款

初始化电子钱包

✓ 计算初始字符串

电子钱包块结构实际上与普通块一样，只不过是按照指定的格式组织后，系统便认为他是电子钱包，能按照电子钱包执行增减值操作。

电子钱包块的存储仅支持整数，所以需要数据进行处理，存储金额时，可以将数值乘以100，以下是电子钱包格式表，以金额100为例（实际上写入的是10000）：

| 金额正 | 金额反 | 金额正 | 区块正 | 区块反 | 区块正 | 区块反 |
|-------------|-------------|-------------|-----|-----|-----|-----|
| 10 27 00 00 | EF D8 FF FF | 10 27 00 00 | 09 | F6 | 09 | F6 |

块地址：0

初始金额：100

X100=

10000

转十六进制

块地址：09

初始金额：10270000

取反

块地址反：F6

金额反：EFD8FFFF

计算写入值

16进制数据：10270000EFD8FFFF1027000009F609F6

按照电子钱包数据的规则组成新的 16 个字节的十六进制值

（7） 写入

ISO14443实验-电子钱包读写实验

实验指导实验参考实验操作

卡ID : D56F91AC

密钥制卡

卡类型 : Philip Mifire-S50 (14443)
实验块 : 扇区2 块1 块地址9 余额 : 100
密钥A : AAAAAAAAAAAAAA 密钥B : BBBB88888888
操作权限 : 验证A或B密钥可读, 验证B密钥才可写, 验证A或B密钥可扣款, 验证B密钥可充值。

密钥A扣款 密钥B充值 密钥A充值 密钥B扣款 初始化电子钱包

计算初始字符串

电子钱包块结构实际上与普通块一样,只不过是按照指定的格式组织后,系统便认为他是电子钱包,能按照电子钱包块执行常数值操作。
电子钱包块的存储仅支持整数,所以需要数据进行处理,存储金额时,可以将数值乘以100,以下是电子钱包格式表,以金额100为例(实际上写入的是10000):

| 金额正 | 金额反 | 金额正 | 区块正 | 区块反 | 区块正 | 区块反 |
|-------------|-------------|-------------|-----|-----|-----|-----|
| 10 27 00 00 | EF D8 FF FF | 10 27 00 00 | 09 | F6 | 09 | F6 |

块地址: 9 初始金额: 100 X100= 10000

转十六进制

块地址: 09 初始金额: 10270000

取反

块地址反: F6 金额反: EFD8FFFF

计算写入值

16进制数据: 10270000EFD8FFFF1027000009F609F6

写入

块地址: 9

写入成功

将计算后的十六进制值写入到块地址为 9 的块区中, 如果提示写入成功, 说明电子钱包制作成功, 如果写入失败可能是没有权限。

注: 如果写入成功后, 制卡信息的块地址信息会改变, 以及金额会发生改变。必须重新操作“密钥 A 扣款”、“密钥 B 充值”、“密钥 A 充值”、“密钥 B 扣款 ”四个操作才能完成该实验。

六、实验思考

思考每个扇区中的控制权限的权限规律, 和初步认识控制位。