

SmartCardStudio 使用手册

通卡行业专业技术工具

5.26.6.27



海南吴信信息系统有限公司

二〇二六年六月

软件版本	版本更新记录
2.17.5.16	创建 V1.0
2.17.9.06	加入 PBOC 和 M1 工具
2.17.9.13	完善密钥分散算法，增加 M1 控制字节生成解析功能
2.17.10.13	加入 4442 卡操作工具
2.17.10.17	优化脚本视图界面，打开脚本自动分配列宽
2.18.04.29	增加加密机配置信息管理
2.18.05.16	增加启动时版本检查与更新，更新 PBOC 计算工具启动数据
2.18.06.23	完善脚本编辑后关闭时的处理逻辑，增加部分厂商链接，修复已知 BUG，致敬劳动者！
2.18.11.24	SocketTest 加入服务器模式
	D8 读卡器的操作兼容 T10 读卡器
5.26.6.6	合并基础库，全面使用 64 位平台编译，优化界面，优化工具栏工具，增加项目目录管理功能
5.26.6.27	新增虚拟卡功能、APDU 生成功能、脚本模块管理功能，如果您喜欢本软件，欢迎打赏，感谢您的支持，您的认可，是我们持续更新的动力。

目录

第一部分：脚本编写	1
一、变量定义	1
1、系统变量	1
2、用户变量	1
3、使用要求	1
二、函数	1
1 @reset	1
2 @stop	1
3 @strmid	2
4 @strmidh	2
5 @compare	2
6 @setreader	3
7 @setslot	3
8 @strlen	3
9 @strlenh	4
10 @des	4
11 @descbc	4
12 @mac	5
13 @Xor	5
14 @ASC2HEX	5
15 @HEX2ASC	6
16 @SUBKEY	6
17 @RSAPUBENC	6
18 @HASH	7
三、综合示例脚本	7
第二部分：软件系统使用	11
一、系统安装与注册	11
1、数据文件说明	11
二、系统功能介绍	12
1、菜单	12
2、系统工具栏	13
3、指令工具栏	15
4、脚本视图	16
5、脚本编辑器	17
6、辅助工具	17
7、项目管理	18
第三部分：附加工具	19
一、加解密工具	19
1、DES 计算	20
2、AES 计算	21
3、MAC 计算	22
4、HASH 计算	23

5、RSA 计算	23
6、CRC 计算	24
7、文本转换	25
8、XOR 异或计算	26
二、PBOC 计算工具	27
1、密钥分散	27
2、MAC\TAC 计算	27
三、M1 测试工具	28
四、TLV 解析工具	29
五、TAG 管理工具	30
六、SOCKET 接口测试工具	31
1、选项说明	31
2、服务器模式	31
七、4442 卡操作工具	32
1、工具路径	32
2、操作	32
3、4442 卡规范	32
八、USR-TCP232-Test	33
九、虚拟卡	34
十、APDU	35
十一、脚本模块管理	35
十二、打赏与广告接入	36

第一部分：脚本编写

一、变量定义

1、系统变量

系统保留变量有：

%resp	保存指令执行后的返回值
%sw	保存指令执行状态码，如：9000

2、用户变量

用户可以自行定义脚本变量，定义方法为：%变量名

3、使用要求

变量名与其它变量、常量或函数调用等之间，必须用空格分开。
如：%var1= %var2 %var3 0099

二、函数

脚本支持函数调用，可以通过函数调用完成多种计算功能。
函数调用方式为：@函数名(参数)。

1 @reset

函数功能：读卡器复位
函数原型：@reset()
示例脚本：
@reset()

2 @stop

函数功能：停止脚本运行
函数原型：@stop()

3 @strmid

函数功能：截取字符串中的子串,按字符取。

函数原型：@strmid(%str1,%cbegin,%ccount)

参数说明：

%str1

源串

%cbegin

要截取的子串起始位置

%ccount

要取的长度

示例脚本：

```
%str1=112233445566
```

```
%substr=@strmid(%str1,0,2)
```

4 @strmidh

函数功能：截取字符串中的子串,按字节取(2 字符)

函数原型：@strmidh(%str1,%cbegin,%ccount)

参数说明：

%str1

源串

%cbegin

要截取的子串起始位置

%ccount

要取的长度

示例脚本：

```
%str1=112233445566
```

```
%substr=@strmidh(%str1,0,2)
```

5 @compare

函数功能：要比较的两个数据，与期望一样则返回 TRUE(1)，不一样则返回 FALSE(0)

函数原型：@compare(%strpara1,%strpara2,%except)

参数说明：%strpara1,%strpara2 为要比较的两个值或变量,%except 为期望结果，如果期望两个值相同，则%except=1，如果期望两个值不相同，则%except=0

示例脚本：

```
%strpara1=9000
```

```
00A40000023F00
```

```
@compare(%strpara1,%resp,1)
```

```
@compare(%sw,6a81,1)
```

6 @setreader

函数功能：设置后面指令要发送到的读卡器

函数原型：@setreader(%reader)

参数说明：%reader 为读卡器在读卡器列表中的索引

示例脚本：

```
%psamreader = 0
%userreader=1
@setreader(%psamreader)
@reset()
@setreader(%userreader)
@reset()
```

7 @setslot

函数功能：设置后面指令要发送到的读卡器卡槽

函数原型：@setslot(%slot)

参数说明：%slot 为读卡器的卡槽参数，具体参数参考下表：

读卡器类型	卡槽参数说明
德卡 D8	用户卡 0x00 侧卡槽 0x0C SIM1 0x0D SIM2 0x0E SAM3 0x0F
德卡 D6	用户卡 0x01 左边 PSAM 卡 0x11 右边 PSAM 卡 0x12

示例脚本：

```
;D8
%userslot = 00;
%psamslot = 0D;
;用户卡复位
@setslot(%userslot)
@reset()
;PSAM 卡复位
@setslot(%psamslot)
@reset()
```

8 @strlen

函数功能：获取字符串的长度，单位为字符

函数原型：@strlen(%str)

参数说明:

%str

要获取长度的字符串

示例脚本:

9 @strlenh

函数功能: 获取字符串的长度, 单位为字节, 1 字节为 2 字符

函数原型: @ strlenh (%str)

参数说明: %str 要获取长度的字符串

示例脚本:

10 @des

函数功能: 使用 DES 算法加解密数据

函数原型: @des(%sKey, %sData, %iMode)

参数说明:

%sKey

密钥, 长度可以为 8 字节, 16 字节和 24 字节。如果密钥长度为 8 进行单 DES 计算, 如果密钥长为 16 进行 3DES 计算

%sData

数据。

%iMode

加解密标志, %iMode=0 加密, %iMode=1 解密。

示例脚本:

```
%sesloaddata = %lrnd %jyxh 8000
```

```
%seslk = @des(%dlk,%sesloaddata,0)
```

11 @descbc

函数功能: 使用 DESCBC 算法加解密数据(CBC 模式 DES 算法) 如果密钥长度为 8 进行单 DES 计算, 如果密钥长为 16 进行 3DES 计算。

函数原型: @DesCBC(%sKey, %sData, %sInitvector, %iMode)

参数说明:

%sKey

密钥, 长度可以为 8 字节, 16 字节和 24 字节。

%sData

数据。

%sInitvector

初始值, 一般为 0000000000000000。

%iMode

加解密标志, %iMode=0 加密, %iMode=1 解密。

示例脚本:

12 @mac

函数功能: 计算 MAC 值

函数原型: @mac(%key,%data,%init,%mode)

参数说明:

%key

计算 MAC 时使用的密钥

% data

需要计算 MAC 的数据

% init

计算 MAC 时使用的初始向量, 一般为 8 字节 00 或 CPU 卡取的随机数

% mode

为 1 时返回 4 字节 MAC, 为 0 时返回 8 字节 MAC

示例脚本:

```
%jmeploaddata=%jyje 02 %termno %transtime 800000000000
```

```
%eploadmac2=@mac(%seslk,%jmeploaddata,%rand,1)
```

13 @Xor

函数功能: 逻辑运算函数, 计算异或

输出长度和%sInit 相同, %sInit 默认为 00, 即逐个字节进行逻辑运算。如果%sData 长度不为%sInit 的整数倍, 在其后自动补 00。

函数原型: @Xor(%sData, %sInit)

参数说明:

%sData

要进行运算的数据, 十六进制形式表示。

%sInit

用来运算的数据, 十六进制形式表示

示例脚本:

```
;结果为 11
```

```
<--! %sxor=@xor(112233445566778899, 00)
```

```
;结果为 9988
```

```
<--! %sxor1=@xor(112233445566778899, 0000)
```

14 @ASC2HEX

函数功能: 将 ASCII 字符串转为 HEX 码字符串, 如: 00 转为 3030

函数原型: @ASC2HEX(%str)

参数说明:

%str

要转换的 ASCII 字符串

示例脚本:

15 @HEX2ASC

函数功能: 将 HEX 字符串转为 ASCII 字符串, 如: 3030 转为 00

函数原型: @HEX2AS(%str)

参数说明:

%str

要转换的 HEX 字符串

示例脚本:

16 @SUBKEY

函数功能: 对密钥进行分散, 产生子密钥

函数原型: @SUBKEY(%KEY,%SN)

参数说明:

% KEY

要分散的主密钥, 分散后的密钥长度由主密钥决定

% SN

分散因子, 分散级数由分散因子 sn 决定, 每 8 字节为一级分散, 第一次分散的在前, 最后一次分散的在最后

示例脚本:

17 @RSAPUBENC

函数功能: 使用公钥对数据进行加密, 用户卡中的公钥是使用机构私钥签名过, 使用公钥加密即可获取明文

函数原型: @RSAPUBENC(%n,%e,%data)

参数说明:

%n

公钥模

% e

公钥指数, 一般为“3”

示例脚本:

```
%rsan =
E0A6D801C384B67684936E8CB9387C962DABD20BFCD05B8B4A6AD85D2F23E7D061EE462EC76328012A96F93
5D9135EE9E54402141F787A0978F179A9656859147C5BD4638C8DE582434701487E8F93E2ED14206B3C7820D
E86FB1177C5BA5FECA8D59F58FF9889E785F88969828E52F9798038EAC707D2CEA994F3A50C75454337EA4710
0485C92FAC8EB1C11735C63881B8238C5EB1C0F30D77386F6FDB9461F4DD75E49B395A79ECD40813F68E8861
%rsae = 3
%rsadata =
CE7A0D36CBFE4A42D5BEC32643AB6AC93F5AD6A5C0EC4AFACA950E764984189A058DA85EAB3FD784CCFD25
8FF1275BC9572A126728BAC41AD6579A6FCC1CE30A4B7A749745D67D8F86EFD39E4D1DA7A9D7CBEAC6115C
F90A1FFDAB2348951D14636D8F4C84409A9F31BC544424287DE607C0A15BB835C21D416E14035DAD9D622EE
A50215DEED5FD7F668560F34868678F5E1493BCCED1C48C57560AD8F0E3B5380A959E19719989410A198F291
7004E
%RSAPUB = @RSAPUBENC (%rsan, %rsae, %rsadata)
```

18 @HASH

函数功能: 计算数据的 HASH 值, 使用 SHA1 算法

函数原型: @HASH(%data)

参数说明:

%data

要分散的主密钥, 分散后的密钥长度由主密钥决定

示例脚本:

```
%data=046230516013104380420F0226198E1001019001C4559CCE9543CB442110FBED9B909FDAECED8B
079A8B520A74AC2842A45AB1AEA4BA9B4E2CD2DE577745E6B278249B59F53D2A32151EA9197DDCD4D07D98
5E813F1A3ECD1294181DC4EF1D36425959F37743AFE751241F44855C19EDA6536C490DD3CD7A51C8C6CF967
65AB0BDE08561E05B60A566E76A0BD05FE137BCBCB3EA5017ED9FBF2818ECE64C54A920FBB70D035F240326
02285A0A6230516013104380420F9F0702FF008E0C00000000000000001E031F009F0D05DC603CA8009F0E050
0108000009F0F05DC683CF8005F280201568C1B9F02069F03069F1A0295055F2A029A039C019F37049F21039F
4E148D1A8A029F02069F03069F1A0295055F2A029A039C019F37049F21039F080200307C00
%datahash = @HASH(%data)
```

三、综合示例脚本

```
;;;;;;;;;;;;;;用户卡操作
@setreader(3)
@setslot(%userSlot)
;用户卡复位
@reset()
00a4000002 3f00
```

```

;;;;;;;;;;;;;;选择互联互通应用
00A4040009A00000000386980701
;;;;;;;;;;;;;;读取卡号
00B0950C08
%csn = %resp
;;;;;;;;;;;;;;加密机测试
@setreader(0)

%cck = FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF

%sjlcmd = 0044
@ASC2HEX(2UFD000101000004010203040404030201100000000000000000102030405060708)
;;发送到加密机 1
%sjlcmd
;;比较加密机返回的状态码，是否为正确
%sjlstate = @strmidh(%resp,2,2)
@compare(%sjlstate, 3256 ,1)
;加密机返回数据
%sjlDate = @HEX2ASC(@strmidh(%resp,4,64))
%keyplain = @des(%cck,@strmidh(%sjlDate,7,24),1)
%EK = @strmidh(%keyplain,4,16)

;;;;;;;;;;;;;;已测试成功脚本—————电子钱包圈存
;以下为三个变量赋值：
;分别是终端机编号%termno，终端序号%termxh，交易时间%transtime,
%termno=00 00 99 00 05 01
%transtime=20140714092000

;电子钱包圈存密钥 用工具生成密钥数据脚本文件
;%dlk = EF6E9BDF6898292357204FB976E6ADBC
;%dtk = 01CD6E75DA37E3F8D6FE2332F1B66ED5
;;;;;;;;;;;;;;切换到用户卡
@setslot(00)
@reset()
;交易初始化、交易、取交易验证码。交易类型 01-07 只有一条 tac 密钥，其标示为 0
;选择互联互通应用
00A4040009A0000000038698 0701

;校验 PIN 1234
0020000002 1234

;读余额
80 5C 00 02 04

```

```
;电子钱包圈存
%dlkid=01
%jyje=00 00 01 00
80 50 00 02 0B %dlkid %jyje %termno
%oldbal = @strmidh(%resp,0,4)
%jyxh = @strmidh(%resp,4,2)
%keyver = @strmidh(%resp,6,1)
%desid = @strmidh(%resp,7,1)
%lrand = @strmidh(%resp,8,4)
%mac1 = @strmidh(%resp,12,4)
```

```
;使用圈存密钥生成过程密钥，DLK 对伪随机数||EP 联机交易序号||8000，加密得到过程密钥
%sesloaddata = %lrand %jyxh 8000
%seslk = @des(%dlk,%sesloaddata,0)
%rand=0000000000000000
```

;计算 MAC1，使用过程密钥对 EP 余额(交易前)4 字节||交易金额 4 字节||交易类型 1 字节||终端机编号 6 字节

```
%mac1data=%oldbal %jyje 02 %termno 80
%ploadmac1=@mac(%seslk,%mac1data,%rand,1)
```

```
;比较计算的 MAC1 与圈存初始化返回的 MAC1 是否一致
@compare(%ploadmac1 , %mac1,1)
```

;计算 MAC2，使用过程密钥对交易金额 4 字节||交易类型 1 字节||终端机编号 6 字节||交易日期 4 字节||交易时间 3 字节

```
%jmeploaddata=%jyje 02 %termno %transtime 800000000000
%ploadmac2=@mac(%seslk,%jmeploaddata,%rand,1)
```

```
80 52 00 00 0B %transtime %ploadmac2
%tac = %resp
```

```
;读余额
80 5C 00 02 04
```

;校验 TAC 说明：TAC 左 16 字节与右 16 字节异或，得到过程密钥，如 DTK=73C4515D673104610E0D19199B4AE926，过程密钥为:7DC94844FC7BED47

;计算 TAC，使用过程密钥对 EP 余额(交易后)4 字节||EP 联机交易序号(交易前)2 字节||交易金额 4 字节||交易类型 1 字节||终端机编号 6 字节||交易日期 4 字节||交易时间 3 字节计算 MAC

;如：过程密钥为:7DC94844FC7BED47，数据为 000027130000000027130211223344556620140714102829，得到 9BB8236C

```
%tacdata = @strmidh(%resp,0,4) %jyxh %jyje 02 %termno %transtime 8000000000000000
%tackey = @xor(@strmidh(%dtk,0,8),@strmidh(%dtk,8,8))
%taconline = @mac(%tackey,%tacdata,%rand,1)
;比较计算的 TAC 与圈存返回的 TAC 是否一致
```

@compare(%taconline , %tac,1)

;读电子钱包圈存明细（001A）

00 B2 01 D4 17

;电子钱包交易明细记录文件（0018）

00 B2 01 C4 17

第二部分：软件系统使用

一、系统安装与注册

本软件下载即可使用，目前对广大用户免费开放，感谢您的支持，如有疑问，可以发送邮件到：

[技术咨询：taozhigao@hxinsys.com](mailto:taozhigao@hxinsys.com)

1、数据文件说明

1.1、SmartCardStudio.ini

本数据文件保存系统运行的配置和相关参数数据，软件更新或卸载时，建议先备份到其它目录保存。

1.2、脚本

脚本是系统使用期间用户自己生成的功能和项目性文件，建议软件更新或卸载时，先备份到其它目录保存。

1.3、dictdata.bin

TAG 标签管理工具软件使用的数据文件，如果有做过编辑，建议软件更新或卸载时，先备份到其它目录保存。

二、系统功能介绍



本软件系统主要为用户提供智能 IC 卡的测试服务，用户不用关注加密机、读卡器等设备的连接编码，通过本软件即可编写脚本实现卡的功能测试。

软件系统提供加解密计算、PBOC 计算、TLV 解析、M1 卡测试(仅 D8 读卡器)、4442 卡测试(仅 D8 读卡器)等一系列辅助工具，方便用户测试。后续将陆续推出标准化测试等服务，方便用户间通过系统来实现知识共享与沟通。

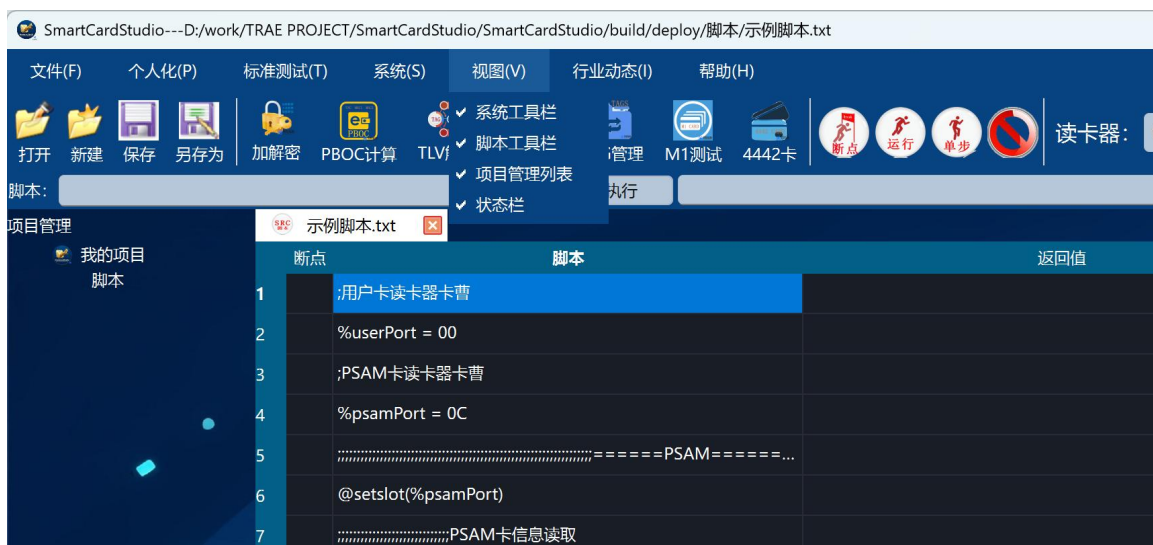
如果您对我们的软件满意，可以扫一扫软件右下角的打赏码，向开发者表示一下支持，谢谢！您在使用过程中有什么意见，可以通过邮箱反馈，我们会及时处理。

1、菜单



系统提供的菜单功能，目前主要是脚本运行与软件辅助功能。

1.1、视图



通过视图菜单的选择，可以显示或隐藏界面视图项。

1.2、帮助



开发文档：打开使用手册，可以了解系统使用方法及脚本规范。

访问我们：查询我们官方网站，获取更多资讯。

系统更新：下载最新版本系统安装包。

关于：查看正在使用的系统版本信息。

2、系统工具栏



系统工具栏提供常用工具按钮，包括脚本打开、脚本新建、脚本执行、读卡器选择、读卡器操作、常用辅助工具等，鼠标移动到按钮上可以获得相应的提示信息。

2.1、脚本功能

脚本执行功能分为：



F5，从脚本视图中的选择的高亮行开始，执行到断点处脚本即停止执行



F8，从脚本视图中的选择的高亮行开始执行脚本，执行脚本过程中，忽略

断点



F10，单步执行脚本视图中选择的高亮行



SHIFT+F5,脚本自动运行过程中可停止脚本运行

2.2、设备操作功能



打开选择的读卡器(连接加密机)



对打开的读卡器进行复位操作(加密机无实际操作)



关闭选择的读卡器连接

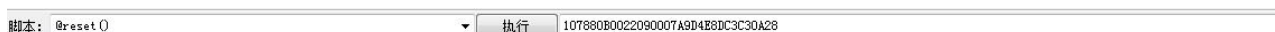
特殊说明：

当选择的读卡器为加密机时，打开操作将会打开加密机的配置对话框，如下图：



可以通过加密机名选择以前使用过的加密机配置，也可以直接进行修改配置使用，点击确定后，系统将保存加密机配置。

3、指令工具栏



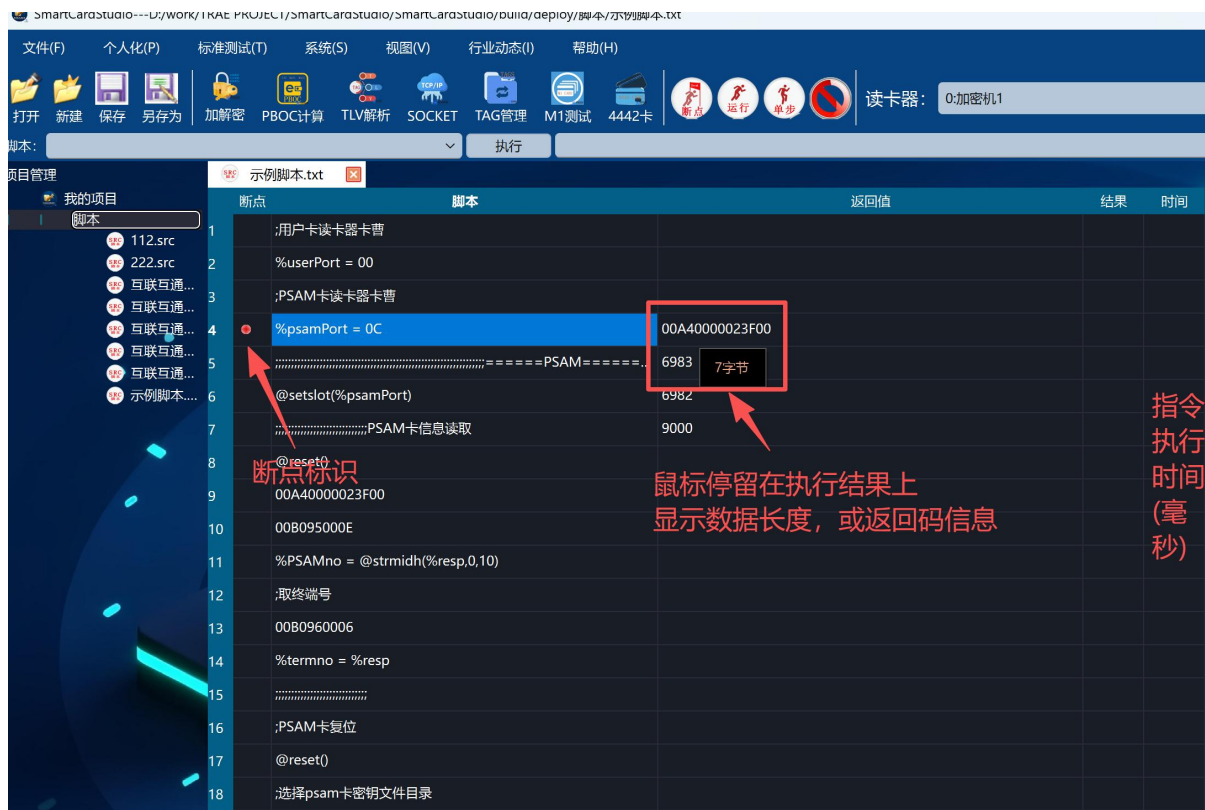
用于单独执行一条临时的指令，点击“执行”按钮后，执行结果在按钮后面的文本框中显示。

操作小技巧：

在工具栏中点击右键，可以弹出工具栏显示、隐藏的控制菜单



4、脚本视图



在脚本视图中，点击需要断点的行中的断点列，即可在脚本中加入或删除断点，对脚本列的编辑也可以保存到脚本文件中。

当指令执行失败时，鼠标停留在返回值上，系统即可提示失败信息，如：卡返回 6982，系统提示“安全状态不满足”。

操作小技巧：

双击“脚本”“返回值”列头后面的分隔线



视图将该列的列宽自适应为该列最大数据长度的显示宽度。

当打开多个脚本时，鼠标停放在脚本标题上，通过滑动鼠标的滚轮，可以快速切换脚本；双击标题，可以快速关闭脚本。

5、脚本编辑器



新建脚本后可以编辑，也可以在打开的脚本中(脚本视图)进行编辑然后保存。
如果关闭时存在未保存的修改，系统将进行提示保存。

6、辅助工具



附加工具在工具栏中可以快速启动使用。

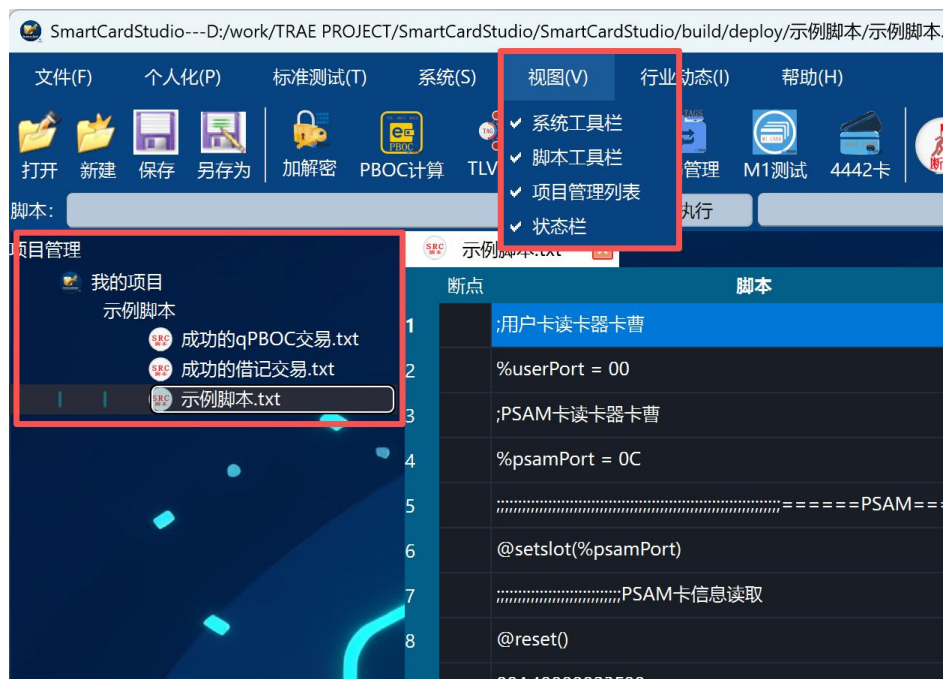
操作小技巧：

在系统菜单的辅助工具菜单中，可能会存在更多实用但不常用的工具，有空记得去看看……



7、项目管理

项目是以管理项目目录的形式进行管理，在视图菜单中打开项目管理列表，即可看到界面左边的项目管理列表信息，在“我的项目”上点击右键可以将项目目录添加进来，在项目目录上点击右键，可以删除项目目录。



第三部分：附加工具

一、加解密工具

加解密工具-吴信信息

DES/3DES AES MAC HASH RSA 文本转换 XOR CRC

模式: DES ECB

密钥:

IV: 0000000000000000

数据:

结果:

加密 解密 分散子密钥

DES算法ECB模式:密钥长度为8字节,不使用初始向量,数据长度为8字节的倍数

支持通卡行业常用的算法，并提供文件转换、CRC、异或等功能。

1、DES 计算



加解密工具-吴信信息

DES/3DES AES MAC HASH RSA 文本转换 XOR CRC

模式: DES ECB

密钥:

IV: 0000000000000000

数据:

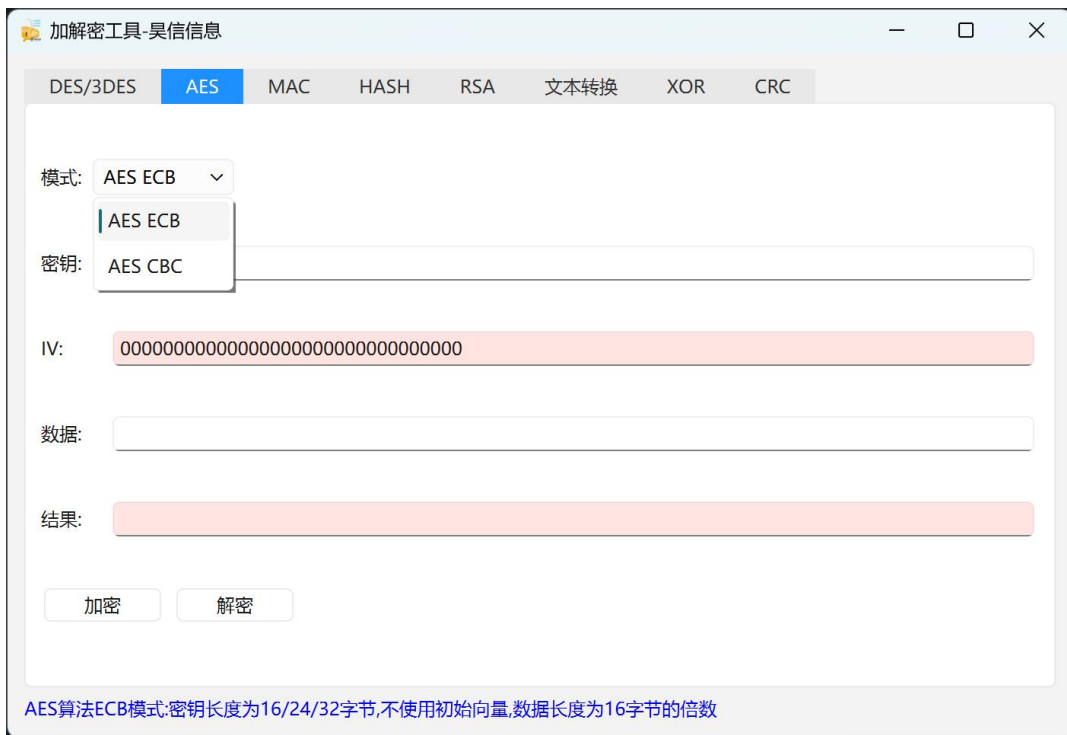
结果:

加密 解密 分散子密钥

DES算法ECB模式:密钥长度为8字节,不使用初始向量,数据长度为8字节的倍数

输入密钥和计算数据后，根据密钥长度选择相应的算法，然后点击需要进行的计算按钮(加、解密、分散子密钥)，选择算法后，算法标题上方有相应的数据和算法要求提示。

2、AES 计算



加解密工具-吴信信息

DES/3DES AES MAC HASH RSA 文本转换 XOR CRC

模式: AES ECB

密钥: AES CBC

IV: 00000000000000000000000000000000

数据:

结果:

加密 解密

AES算法ECB模式:密钥长度为16/24/32字节,不使用初始向量,数据长度为16字节的倍数

与 DES 算法一样，输入计算的密钥和数据，并选择算法，然后点击需要计算的按钮

3、MAC 计算



加解密工具-吴信信息

DES/3DES AES **MAC** HASH RSA 文本转换 XOR CRC

算法: CBC-MAC (16字节密钥) 填充方式: 数据不做填充

密钥:

IV: 0000000000000000

数据:

MAC:

计算MAC

CBC-MAC算法:密钥长度为16字节,初始向量8字节,数据长度为8字节的信数

与 DES 算法一样，输入密钥、数据，然后选择算法，其中 CBC 模式 IV 为算法的初始向量值，需要根据具体的业务算法设计进行输入。

4、HASH 计算

加解密工具-吴信信息

DES/3DES AES MAC **HASH** RSA 文本转换 XOR CRC

算法: SHA-1

数据: 0000000000000005E031F009F0D05D8603CA8009F0E0500108000009F0F05D8683CF8005F280201567C00

HASH: AB0444B451F6871E7901DF8D76A70CC5D0064811

计算HASH

SHA-1算法:输入数据任意长度,输出160位(20字节)哈希值

算法支持 SHA1 和 SHA3 算法，如果需要使用 SHA3 算法，选择图中的对应算法即可。

5、RSA 计算

加解密工具-吴信信息

DES/3DES AES MAC HASH **RSA** 文本转换 XOR CRC

密钥长度: 1280 E: 010001

N: 060BFF2F9D32AF205449C129AB5DE975B99658CDE30C0A28899EDA11B66AA4681DB178351108F7E29B

D: 8336E6B632FF27A7CADFC0D173E581D7C62378F4209E142F18CC1DF0FF777D22240159662E320347EC1

P: 16A3FF91ABA2C8DF27629291A05D9699F534B Q: 249E159ABBB8AD04D9353448593AC60ACBF1

dP: D337E66B7E63AE6F978DB dQ: 1B4B05817F5C4F1D2C151 Qinv: FF977727A4E06DBF1FD4F

数据: 9D6239A0DC8BE419A8907A38C3EB05ED4401FEEB422ED02C77E56AFFAEC408EE63A90B6301EA2095
D8D3A7CF8B4E86C17CAF865CEE64B34C62B4772B1DA70AF4F8E6290895325CE7B080C74C7E6527C6
E7B8827672671C60D75117CFDECFD217D22DFFA78380169FFD4E382FB6D79B4C5000775D9A986F3

结果: 17F3BDE5568BDD7A918BD721AA57E1792ED4D4AD5CAFF1049F9722036A3E2A76075F1BDF9157795
40F06CB3F1F1FB38E04CDE5804AEA1358FFA1BEF60C744FD0D4E6877F58EE3B36141A25B39F9B01840
ECD78289EC000F5CFC68DE38158D8413DBCACB992B058F1274F275CECFD6D304F9F582904C25DEF

生成密钥 加密 解密 补齐密钥 检查密钥

补齐密钥需要N、E或D的值 (N,E)是公钥 (N,D)是私钥 N:公钥模数 E:公钥指数 D:私钥指数

RSA算法工具

支持标准的国际 RSA 算法，可以生成密钥，或需要公私钥数据进行加解密运算，输入的数据都

是按 16 进制字节码处理。

6、CRC 计算

加解密工具-吴信信息

DES/3DES AES MAC HASH RSA 文本转换 XOR **CRC**

类型: CRC-16

数据: 12332112321312

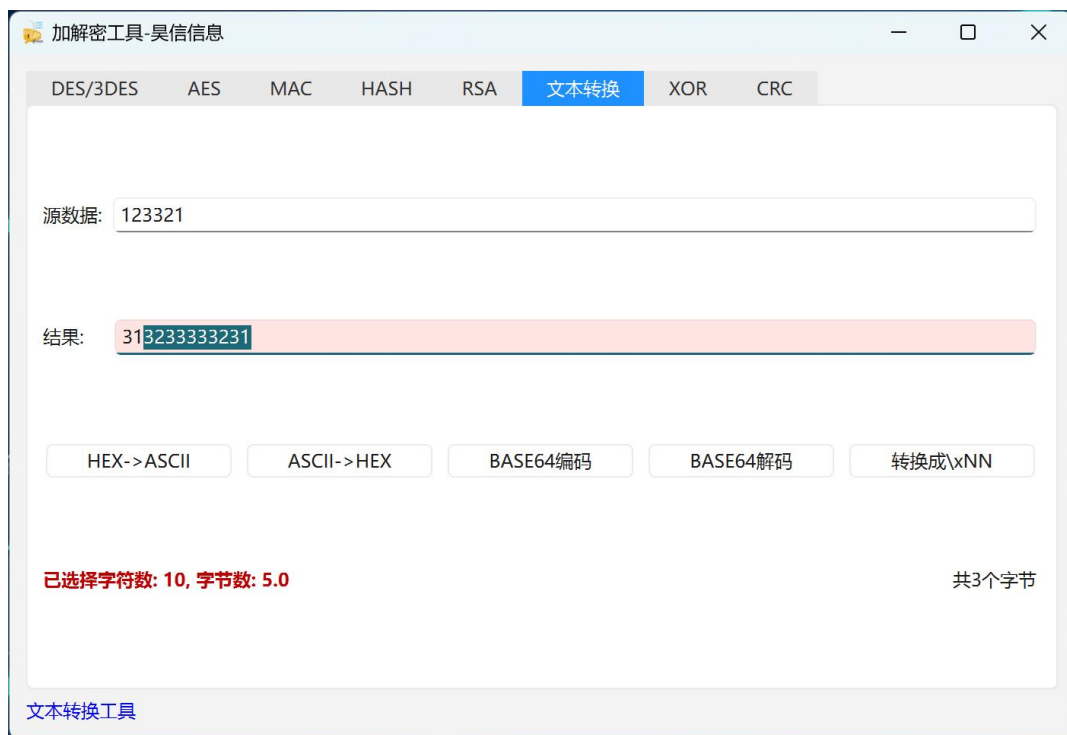
CRC: 4FB9

计算CRC

CRC-16校验:输入数据任意长度,输出16位(4字节十六进制)校验值

循环校验码(CRC 码)的标准计算方法。

7、文本转换



非常实用的编码转换工具，当用户选择原始数据时，可以提示已选择的数据长度。各个功能都比较实用，建议用户试试所有的转换功能，方便找到自己常用的功能。“转换成\xNN”适合编程人员在将脚本写到代码中的使用，直接实现数据拷贝即用。

8、XOR 异或计算



加解密工具-吴信信息

DES/3DES AES MAC HASH RSA 文本转换 **XOR** CRC

数据: 123456

密钥: 112233

结果: 031665

计算XOR

XOR异或运算:数据与密钥按位异或,密钥长度任意,数据长度任意

标准的异或算法。

二、PBOC 计算工具

PBOC计算工具-吴信信息

说明: 输入数据时, 保证输入的数据框不能再输入, 数据才完整, 如果城市代码长度不够16位则不对城市代码分散, 即根密钥为城市密钥

密钥分散

根密钥: 00000000000000000000000000000000 城市代码: 0000000000000000 卡片序列号: 0000000000000000

城市密钥: 8CA64DE9C1B123A7355550B2150E2451 卡片密钥: F48AECDD730A8889AEE4BC377A82A4083

充值计算(交易金额单位: 分, 交易时间(YYYYMMDDHHMMSS))

充值TAC计算

DTK: 00000000000000000000000000000000

余额: 00000000 卡片交易号: 0000

充值金额: 00000000 交易类型: 02

终端号: 000000005566 交易时间: 20170828235028

TAC: CA01DDB8

充值MAC1计算

DLK: 00000000000000000000000000000000

随机数: 1D7D8C32 卡片交易号: 0000

余额: 00000001 充值金额: 00000001

交易类型: 02 终端号: 000000005566

MAC1: EEE1D422

充值MAC2计算

DLK: 00000000000000000000000000000000

随机数: 1D7D8C32 卡片交易号: 0001

充值金额: 00000001 交易类型: 02

终端号: 000000005566 交易时间: 20170828235028

MAC2: F23F8EC9

消费计算

消费TAC计算

DTK: 00000000000000000000000000000000

金额: 00000000 交易类型: 06

终端号: 000000000001 交易序号: 00000000

交易时间: 20170828235028

TAC: 1D7D8C32

消费MAC1计算

DPK: 00000000000000000000000000000000

随机数: 1D7D8C32 卡片交易号: 0000

终端交易号: 4001 金额: 00000001

交易类型: 06 终端号: 000000005566

时间: 20170828235028

MAC1: D3FADF71

消费MAC2计算

DPK: 00000000000000000000000000000000

随机数: C54601AD 卡片交易号: 0001

终端交易号: 4001 金额: 00000001

MAC2: B327FF8F

PBOC计算工具 - 支持密钥分散、TAC计算、MAC计算

支持通卡行业常用的算法计算, 可以帮助用户验证密钥及交易数据校验, 工具有密钥分散算法功能, 用户可以直接计算测试卡对应的卡密钥, 目前支持 2 级分散密钥模式。

1、密钥分散

在界面中输入根密钥, 工具将对密钥使用城市代码分散, 分散结果自动填入“城市根密钥”项中, 当城市代码不够 8 字节时, 不做城市根密钥的分散, 默认根密钥就是城市根密钥; 处理完城市根密钥后, 使用城市根密钥对卡号(CSN)进行分散, 分散结果自动填入“卡片密钥”项中。

2、MAC\TAC 计算

用户在需要计算的项目中输入卡密钥和对应的交易数据, 当数据输入完整后, 将自动计算结果, 并自动填入结果项中。

三、M1 测试工具

读卡器控制

打开读卡器 关闭读卡器 寻卡

密钥管理

密钥: FFFFFFFFFF 加载A密钥 加载B密钥

M1卡读写

读取M1卡 扇区: 0 块: 0 写入块

读取数据:
 写入数据: 00000000000000000000000000000000

卡片信息

ATQA: ATS:
 CSN: SAK:

控制字节分析

控制字节: FF078069 控制字节设置成功

C1	0	0	0	0
C2	0	0	0	0
C3	0	0	0	1
块0	0-禁止	0-禁止	0-禁止	0-禁止
块1	0-禁止	0-禁止	0-禁止	0-禁止
块2	0-禁止	0-禁止	0-禁止	0-禁止
块3	2-KEYB	0-禁止	0-禁止	0-禁止
KEYB	0-禁止	0-禁止		

支持 S50 标准的 M1 卡的读写功能，目前程序支持使用 D8/和 T10 读卡器，用户使用本工具时，请确保读卡器没有被其它程序打开使用；工具还包含有 SAK 注释功能。

工具界面集成有控制字节的生成和解析功能，用于协助用户生成或解析控制字节，控制字节为每个扇区的第三个块，其中 0-2 块为数据块，第 3 块为密码块，第 3 块的第 6、7、8、9 字节为控制字节。用户在调整选项时，可以先选择“查看所有选项”，查看 M1 的控制字节的选项支持情况。用户调整任何选项后，控制字节即时生成，并反馈结果。

数据块 (块 0、块 1、块 2) 的存取控制如下：

控制位 (X=0、1、2)			访 问 条 件 (对数据块 0、1、2)			
C1X	C2X	C3X	读	写	加值	减值, 值转出, 值转入
0	0	0	KeyA B	KeyA B	KeyA B	KeyA B
0	1	0	KeyA B	Never	Never	Never
1	0	0	KeyA B	KeyB	Never	Never
1	1	0	KeyA B	KeyB	KeyB	KeyA B
0	0	1	KeyA B	Never	Never	KeyA B
0	1	1	KeyB	KeyB	Never	Never
1	0	1	KeyB	Never	Never	Never
1	1	1	Never	Never	Never	Never

控制块 块 3 的存取控制与数据块不同, 它的存取控制如下：

C13	C23	C33	密码 A		存取控制		密码 B	
			读	写	读	写	读	写
0	0	0	Never	KeyA B	KeyA B	Never	KeyA B	KeyA B
0	1	0	Never	Never	KeyA B	Never	KeyA B	Never
1	0	0	Never	KeyB	KeyA B	Never	Never	KeyB
1	1	0	Never	Never	KeyA B	Never	Never	Never
0	0	1	Never	KeyA B	KeyA B	KeyA B	KeyA B	KeyA B
0	1	1	Never	KeyB	KeyA B	KeyB	Never	KeyB
1	0	1	Never	Never	KeyA B	KeyB	Never	Never
1	1	1	Never	Never	KeyA B	Never	Never	Never

(KeyA|B 表示密码 A 或密码 B, Never 表示任何条件下不能实现) 控制字节的前三字节为控制位, 第四字节为备用字节, 可随意更改, 只有 B 密码为不可读时第四字节才有效

四、TLV 解析工具

TLV解析--吴信信息

TLV数据: 如 701A61184F08A000000333010101500950424F434445424954870101

解析

701A61184F08A000000333010101500950424F434445424954870101

当前TLV解析出的TAG: (双击查看详情)

TAG: 50

LEN: 09

全局TAG列表: (可双击选择)

VAL:

50424F434445424954

TLV注释:

TAG: 50

LEN: 09

VAL: 50424F434445424954

注释: 应用标签

70

61

4F

50

87

70

61

4F

50

87

添加到构建列表

构建TLV

添加

TAG列表顺序: (双击删除选中的TAG)

TAG:

VAL:

打包TLV

上移TAG

下移TAG

清除子TAG

打包TAG: 70

通卡行业常用的 TLV 数据解析工具, 可以进行解析并提供 TAG 用途注释, 在工具下方可以自行组织生成 TLV 数据。打包 TLV 是将 TAG 列表顺序中的所有 TAG 对应的 TLV, 打包到“打包 TAG”后面对应的 TAG 名称中, 生成一个新的 TLV 数据, 生成结果到待解析的 TLV 数据框中。

五、TAG 管理工具



TAG管理工具-吴信信息

TAG列表

- 9F26
- 9F42
- 9F51
- 9F44
- 9F52
- 9F05
- 5F25
- 5F24
- 94
- 4F
- 82
- 50
- 9F12

TAG: 9F44

格式: n (数字型,1字节, 补位规则: 数据元右对齐, 左补0)

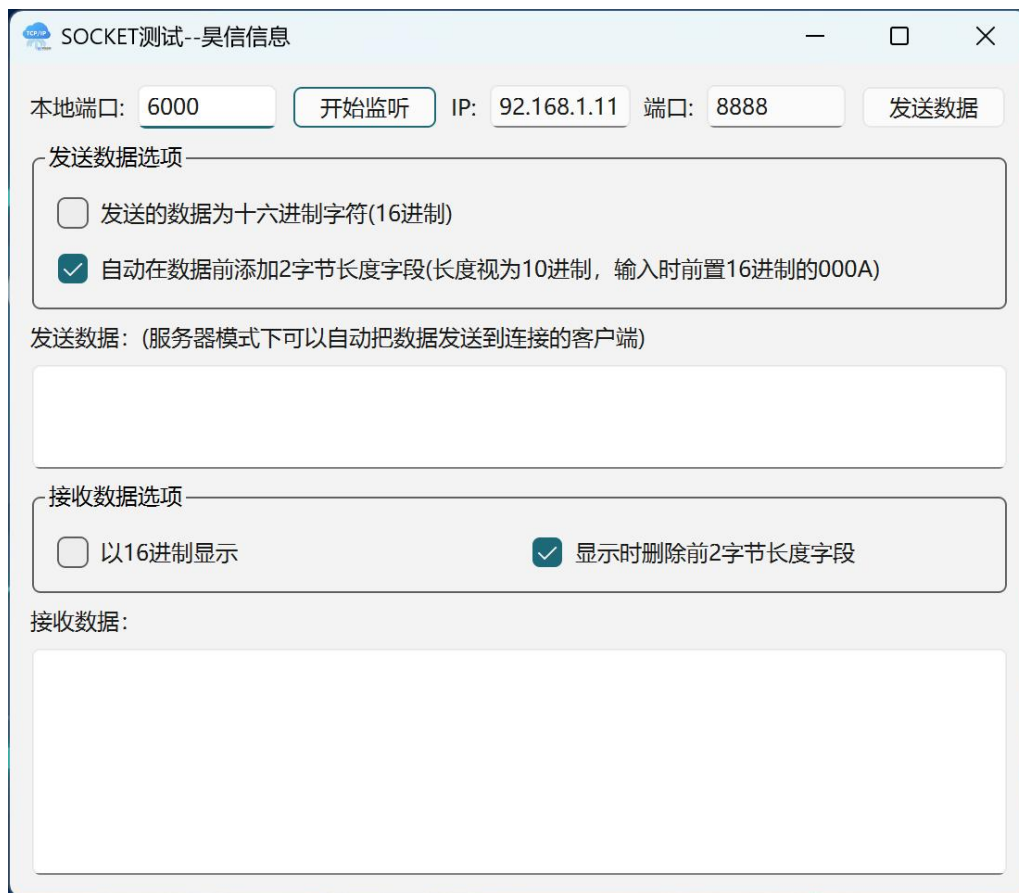
描述: 应用货币指数
--O (可选) : 可选数据元
--指出金额数据中小数点从最右边第几个位置

TAG数量: 170

查找 添加 删除 保存

通卡行业常用的 TAG 标签含意注释工具，支持用户添加自定义 TAG 注释。用户可以在 TAG 后面输入想要查找的 TAG 值，点击查找可以查询库里已包含的 TAG 注释信息，也可以添加新的 TAG 信息数据，修改信息后点击保存，即可更新库中的 TAG 注释信息。

六、SOCKET 接口测试工具



SocketTest 工具可以对 TCP/IP 协议的接口进行测试，例如加密机一般为 TCP/IP 协议，可以通过界面选择，通过 SOCKET 发送 16 进制串或 ASC 码，是否补充长度数据或进行数据转换，请根据发送数据的实际情况进行选择。

1、选项说明

发送的数据为字节码：如果选中，数据框内的数据将不做转换，直接发送；如果不选中，数据框内的数据将先转成字节码形式（BCD 码或 16 进制），然后再发送。

自动在数据前补充 2 字节长度数据：如果选中，系统将计算数据长度(字节数)，然后补充到数据前，再发送。

以 16 进制串显示：将接收的数据(16 进制值)转成 ASCII 后显示出来。

显示时去掉前 2 字节的长度数据：显示数据时，去掉前面 2 个表示长度的字节数据。

2、服务器模式



填写服务器监听端口后，点开始监听，工具即可获取客户端连接，并显示客户端发送的数据。

七、4442 卡操作工具

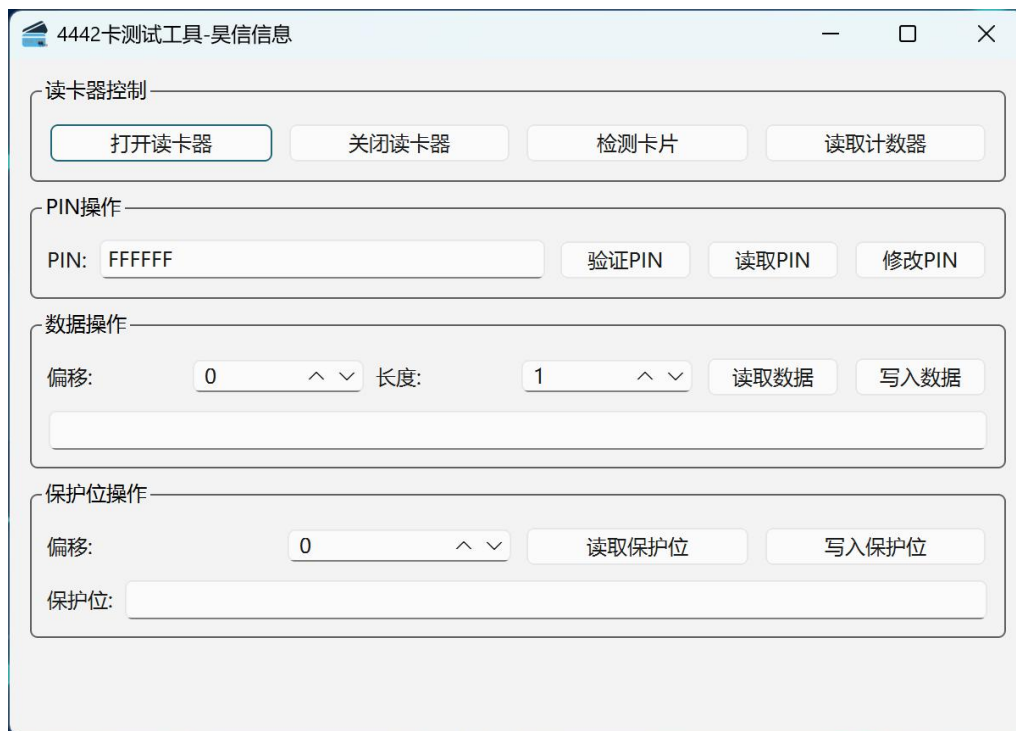
1、工具路径

4442 卡操作工具因不常用，未放入工具栏，打开菜单在系统菜单的系统—>辅助工具—>4442 卡测试



2、操作

4442 卡工具使用 D8 或 T10 读卡器定制开发，可以实现 PIN 操作、数据操作、保护位操作，具体数据设置，可以参考 4442 卡的规范。



3、4442 卡规范

/*****电子性能
256×8 位 EEPROM

字节直接寻址
 低地址 32 字节数据设不可恢复的写保护位
 32 位保护位
 写数据操作结束标志
 符合 7816-3 标准的复位响应
 字节擦除然后写入时间：标准值 25ms
 最少 10000 次的写擦除周期
 数据保存期：10 年

*****/

/*****保密特性

三字节的用户密码。

密码核对正确前，全部数据只可读，不可改写。

核对密码正确后可以更改数据，包括密码在内。

错误计数器，初始值为 3，密码核对出错 1 次，便减 1，若计数器值为 0，则卡自动锁死，数据只可读出，不可进行更改也无法再进行密码核对；

若不为零时，有一次密码核对正确，可恢复到初始值 3。

写保护区（前 32 个字节）的每一字节可单独进行写保护，进行写保护后，内容不可再更改（即固化数据）。

*****/

/*****注意事项

1.除去写保护区的 32 字节，程序员可操作的只有 224 字节,写保护区只有一次写如机会,一般不使用。

2.注意每次改写密码后,只有将卡下电后密码才会生效。

3.密码为 3 字节也就是 24 个位,一般初始密码为“255255255”,转换成 16 进制为六个 F 即“FFFFFF”。

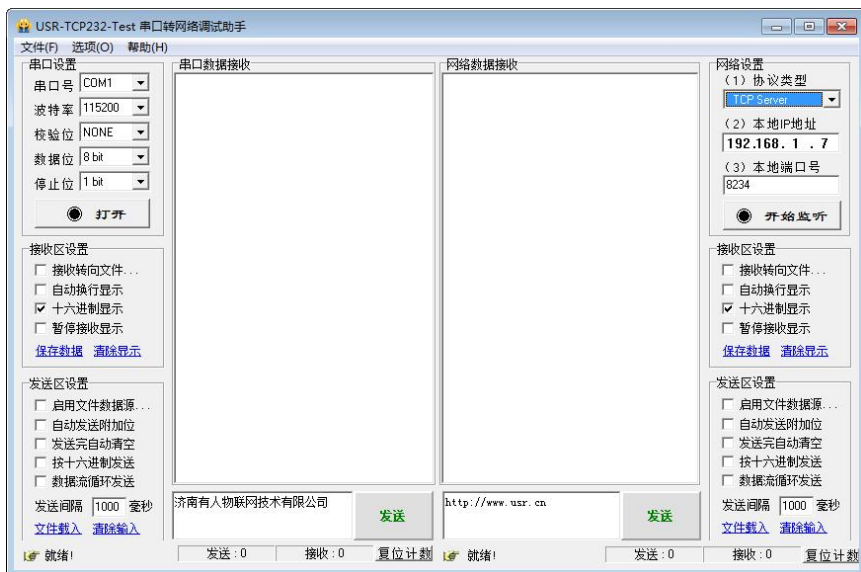
市场上常用的芯片为西门子的 SLE4442，也有使用国产复旦的 FM4442 和 ATMEL 的 AM4442

常应用与酒店门锁及储值卡系统应用

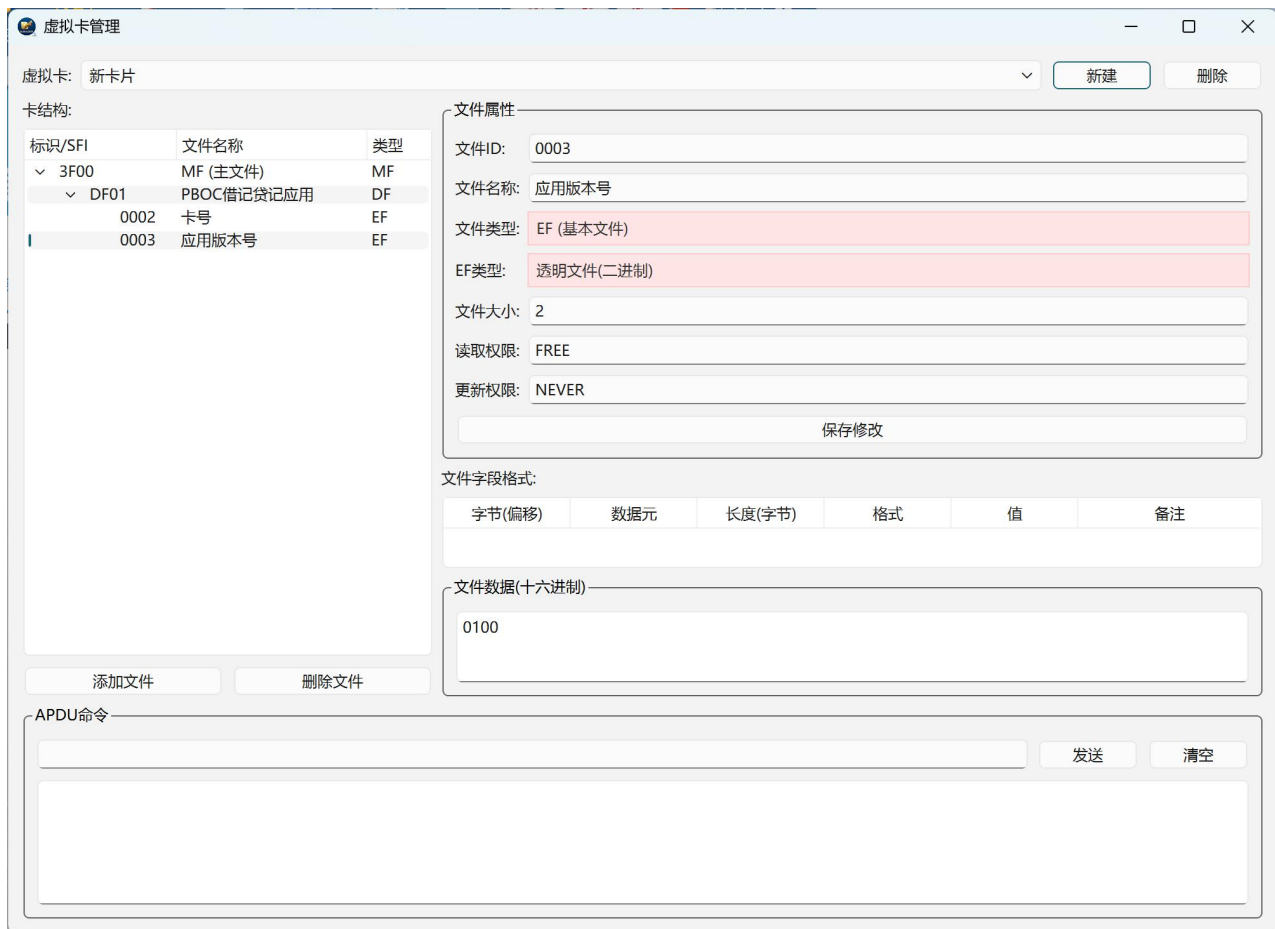
*****/

八、USR-TCP232-Test

USR-TCP232-Test 是一款市场上比较流行的专业串口/网络测试工具，目录软件附带的版本是 V1.3，可以在程序目录下打开 USR-TCP232-Test-V1.3.exe 进行使用。也可以通过菜单中的“系统->辅助工具->USR-TCP232-Test”打开工具。



九、虚拟卡



高级功能菜单下虚拟卡功能。按卡结构规范，配置虚拟卡结构，并测试 APDU 指令功能，本功能初步实现，持续迭代中。

十、APDU

APDU 命令生成器

提示: 1) 选择左侧分组→双击/点击模板加载; 2) 修改 Data 自动重算 Lc; 3) Le 默认空 (不指定响应长度); 4) 浅红色背景为只读字段。

选择分组:

文件操作

指令模板 (双击或单击加载):

- SELECT by File ID (DF)
- SELECT by File ID (MF)
- SELECT by File ID (EF)
- SELECT by AID (应用)
- SELECT PSE (1PAY.SYS.DDF01)
- SELECT MF (补丁)
- SELECT by Path (路径)

APDU 字段 (浅红色为只读)

CLA: 00 INS: A4

P1: 04 P2: 00

Lc: 08 Le: 留空=不指定

Data: A000000333010101

指令说明: [文件操作] SELECT by AID (应用)
按应用标识符(AID)选择应用: P1=04 表示按 AID 选择

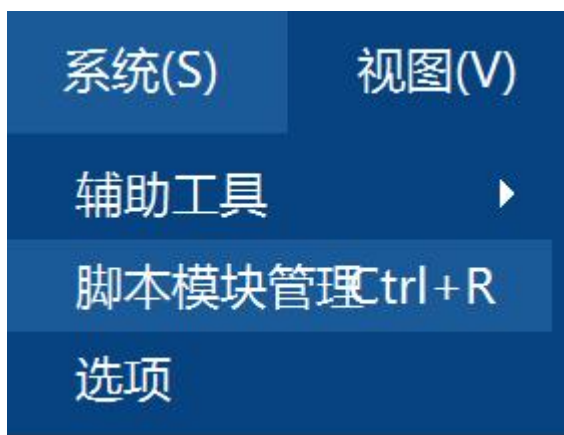
命令预览 (颜色标记各字段)

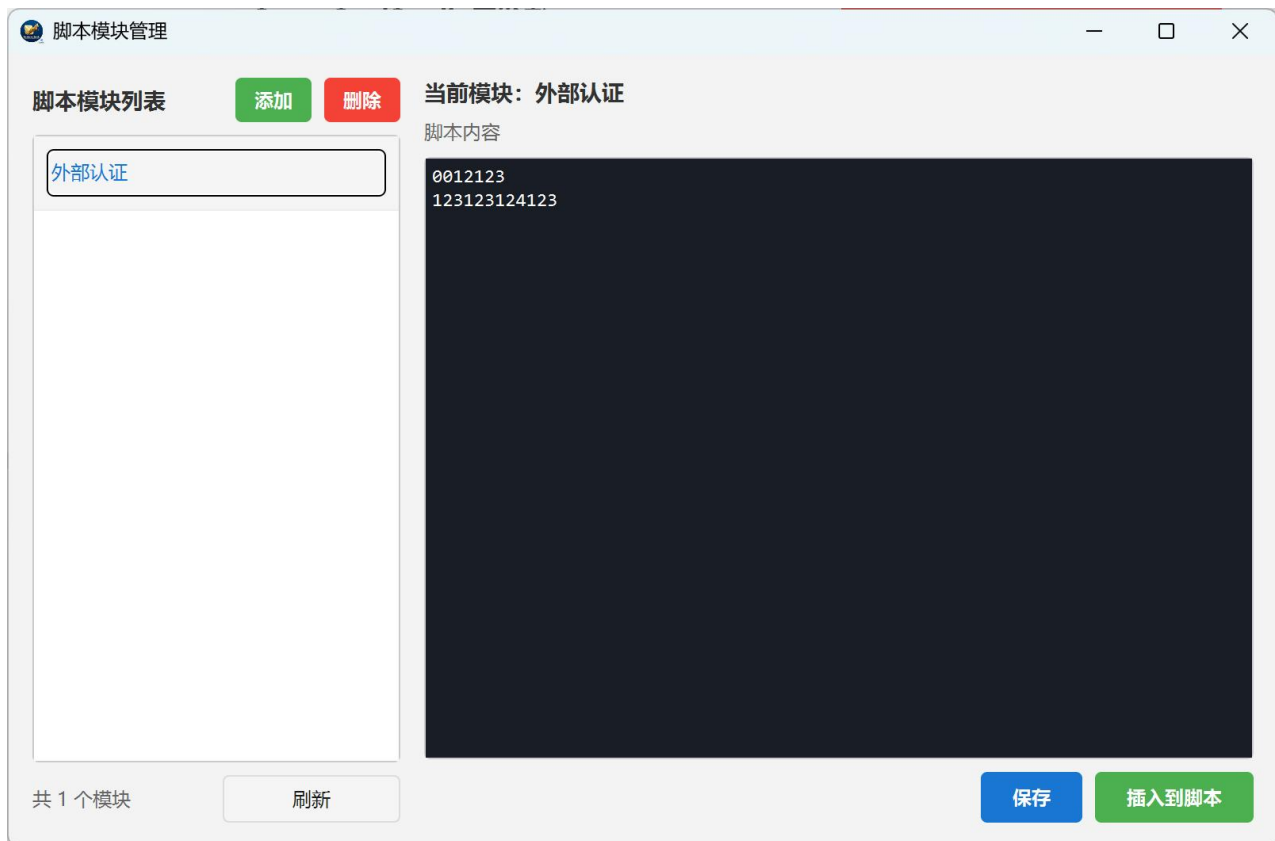
00 A4 04 00 08 A000000333010101

清空 复制命令

高级功能菜单下 APDU 生成工具，常用 APDU 指令的生成和注释，方便用户快速生成 APDU 指令。

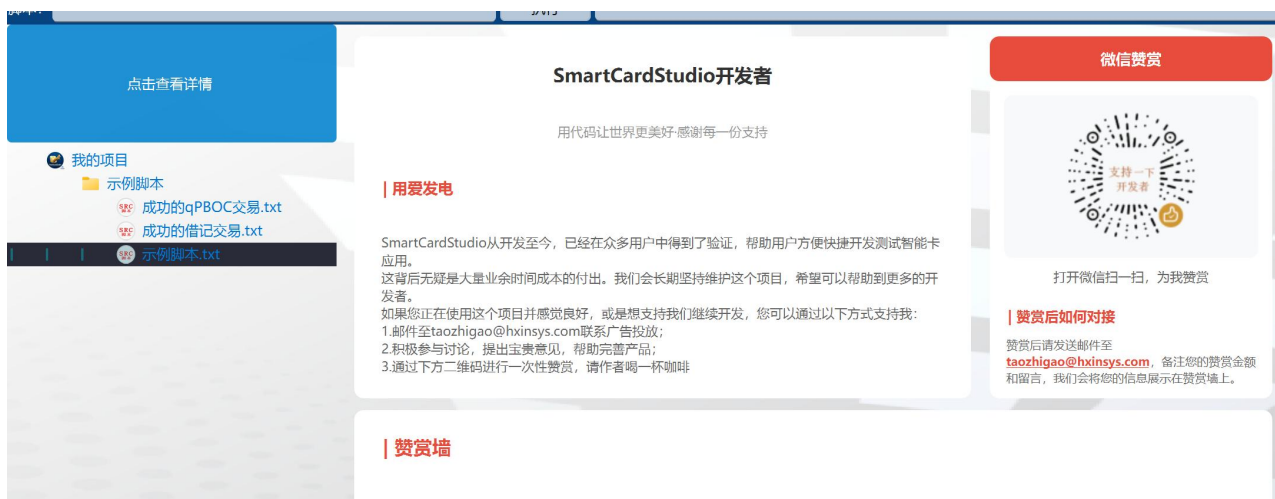
十一、脚本模块管理





方便用户将常用的脚本功能模块化管理，比如充值流程脚本、消费流程脚本等，在编辑完整脚本时，可以直接选择插入到脚本文件中。

十二、打赏与广告接入



为感谢大家的打赏认可，特加入赞赏墙，公示大家的打赏信息，如果您有投放广告的需求，可以邮件联系，如果您打赏了，可以邮件联系我们将打赏信息公示，谢谢。