**SmartCard Plus**

**V4.0.0.0**

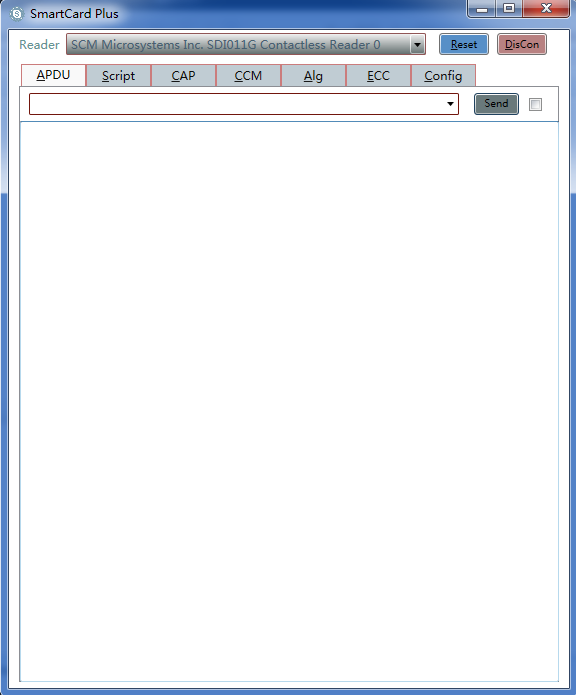
**V2.9**

[**APDU@github**](https://github.com/APDU/SmartCardPlus)

[**map.im**](http://map.im)

## Ⅰ 使用帮助

### 1、Quick Start



发送APDU前应先选择读卡器，并点击Reset按钮;

上图中首字母带下划线的为支持快捷键，使用方式为Alt+首字母，例如Alt+R为复位。

Reader 选择PCSC/CCID读卡器，当选择JCOP Debug时可连接Eclipse JCOP插件;

Reset 连接当前读卡器并复位卡片;

DisCon 断开当前PCSC/JCOP连接;

APDU 发送APDU指令，支持Case1、Case2、Case3、Case4;

Script 执行.lua脚本或者.txt脚本;

CAP 下载cap文件，将cap文件转为APDU;

VIEW 查看/删除卡内应用、安装实例、Put Key、查看卡片空间等;

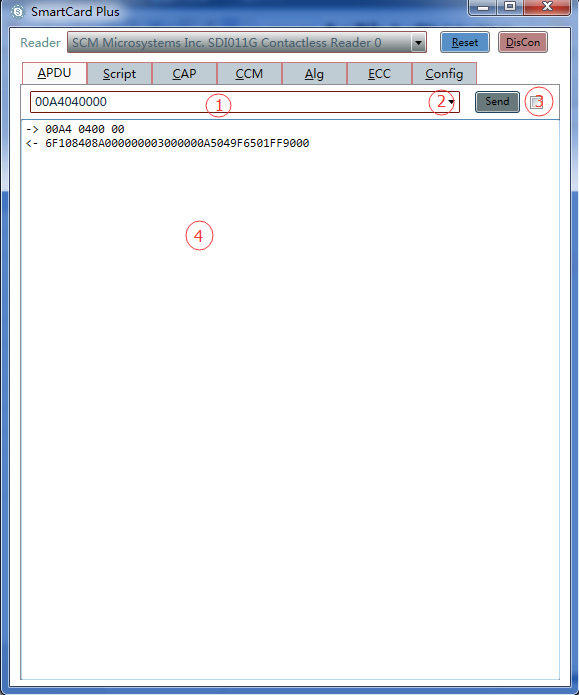
Alg 算法DES/SHA1/SHA2/SHA3/AES/HMAC/SM1/SM3/SM4/Base58/Base64/RSA等;

ECC 椭圆曲线算法ECDSA/SM2;

CFG 软件、卡片GP密钥等配置相关。

本工具支持DM/DAP安全域下的CAP文件下载。

### 2、APDU



1处可以输入APDU指令，可用上下方向键翻滚历史记录，也可按Enter键直接发送APDU

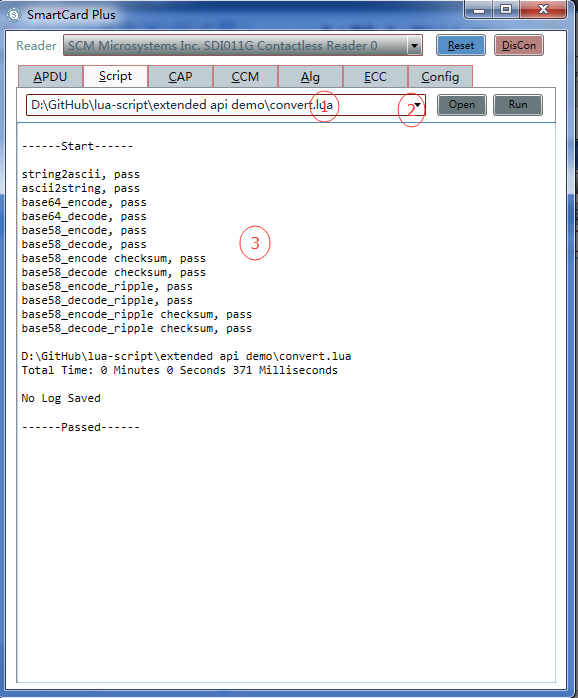
2处的下拉栏可以显示历史记录

Send按钮，点击发发送APDU指令

3处的复选框可自动取响应（当状态字是6CXX/61XX时）

4处用来显示log

### 3、Script



1处可以编辑文件路径，也可将\*.lua或\*.txt直接拖到此处

2处的下拉栏可以显示历史记录

3处用来显示log

Open按钮用来选择脚本

Run用来执行脚本或者停止执行

可以通过Config的log选项来配置是否记录log

Txt脚本(关键字只支持reset、assert、loadkey、auth。不区分大小写)

reset为复位

assert为判断返回值，可以是状态字，也可以是状态字+数据

auth 为打开安全通道，不带任何参数，如果auth前面没有loadkey则默认3支密钥均为404142434445464748494A4B4C4D4E4F, KeyVersion：00, Security level：00

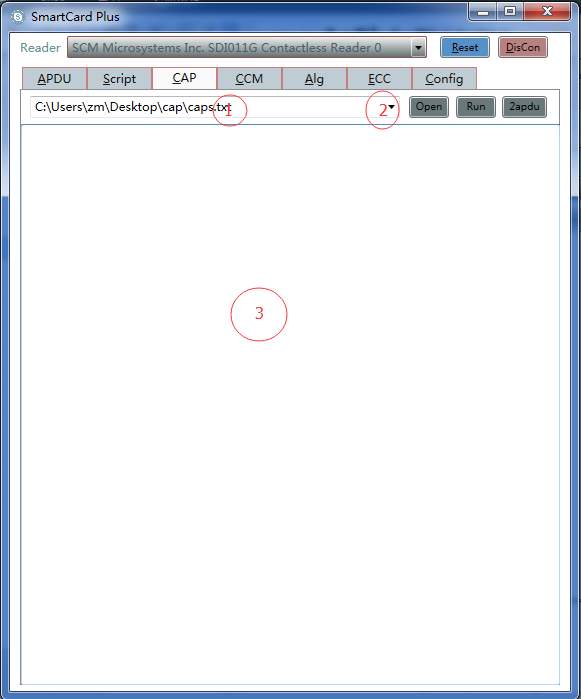
loadkey：参数为Version + Security level + ENC + MAC + DEK

txt格式脚本注释符号为 # 或 //

Lua脚本参见[github](https://github.com/APDU/lua-script)

txt脚本参见

### 4、CAP



1处可以编辑文件路径，也可将\*.cap或者\*.txt拖到此处

2处的下拉栏可以显示历史记录

3处用来显示log

Open按钮用来选择cap文件

Run用来下载cap或者停止下载

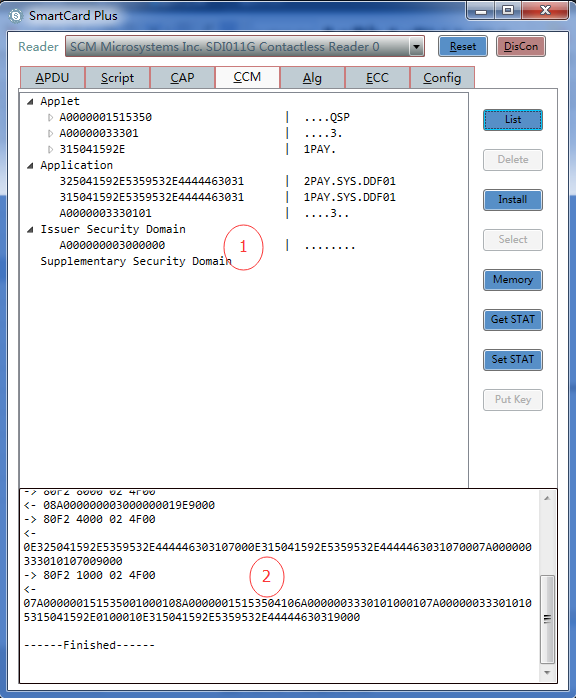
2apdu 将cap文件转为apdu指令流并保存到txt文件中

支持RSA算法的DM,以及RSA/DES算法的DAP安全域下载CAP(需要配置Security Domain中xml的密钥)

可以通过Config的log选项来配置是否记录log

当1处为\*.txt时为批量下载cap包，将\*.txt与cap文件放到同目录下，将cap文件名及后缀按顺序加到\*.txt文件，可参考[我的github](https://github.com/APDU/SmartCardPlus/tree/master/application/cap)

### 5、CCM



1处 显示卡片上已有的应用/安全域

2处 显示log

List列出卡上所有的应用

Delete删除某个或者某组应用，当选中Applet/Application/Issuer Security Domain/ Supplementary Security Domain时可删除该分组下的所有应用

Install安装实例

Put Key在选中某个安全域下才可以操作

Select选中某个AID后发送选择指令

Memory查询卡片剩余空间

Get STAT 获取卡片生命周期

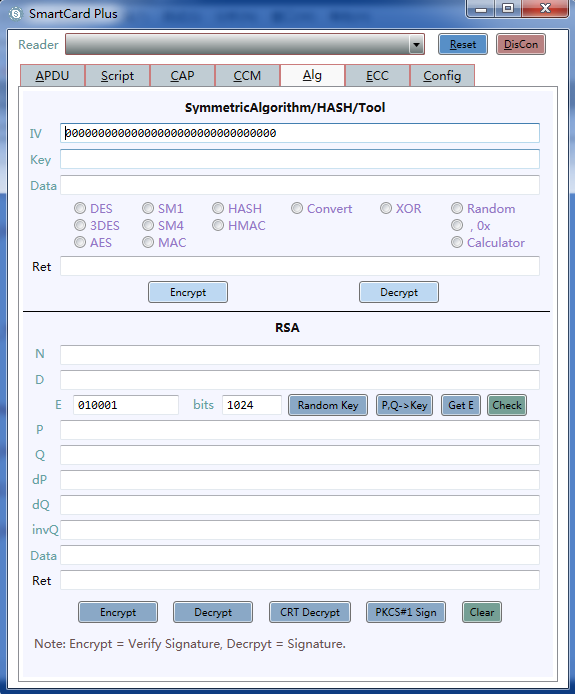
Set STAT 设置卡片生命周期

生命周期转换顺序为：OP\_Ready->Initialized->Secured->Locked

例如：当前状态为Initialized，则变为Secured，依次类推。

如果当前周期为Locked，则设置为Secured。

### 6、Alg



算法均不补任何数据，如果要补数据请手动补

MAC，Data不补任何数据(Pad为强制补80)

XOR，异或

Convert， ASCII/Base58/Base64转换

Random每点击一次Gen按钮可产生8字节随机数

rsa算法支持16-16384bit模长，产生密钥之前请先指定E的值。

Random Key根据E及bits产生随机的密钥

PQ ->Key 根据P、Q、E产生密钥

HASH/HMAC可计算大文件或者HEX字符串的hash

SM1：CBC与ECB模式依赖算法卡，算法卡指令须如下：

sm1 ecb enc：

80320000 lc 90 round data key //data为16字节，key为16-32字节

sm1 ecb dec：

80320000 lc 91 round data key //data为16字节，key为16-32字节

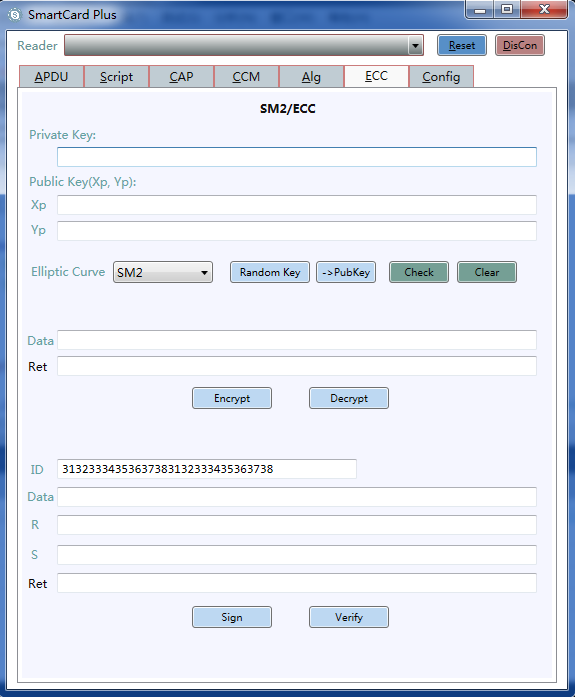
sm1 cbc enc：

80340000 lc 90 round data icv key //icv、data为16字节，key为16-32字节

sm1 cbc dec：

80340000 lc 91 round data icv key //icv、data为16字节，key为16-32字节

### ECC



Random Key 根据曲线类型产生密钥

->PubKey 根据私钥及曲线类型推导公钥

Check为公钥验证

SM2/ECC均不补任何数据

SM2加解密 采用C=C1C3C2 新版本的国密SM2算法

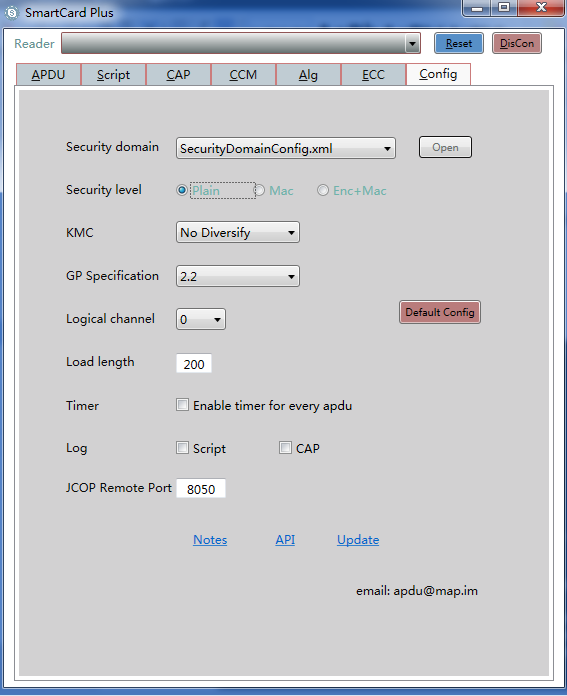
ID为SM2签名验签所需要的标识,ECC不需要

SM2/ECC密钥及加解密数据都未补PC码

SM2加解密、签名验签时输入数据为明文值（无需HASH等）

由于ECDSA签名、验签可以有多种HASH，故输入数据建议为Hash之后的e值

### 8、CFG



Security Domain卡片安全域配置相关，主要是安全域密钥、token密钥、dap密钥等，文件位于exe目录下

KMC 安全域密钥的分散方式

GP Specification不同的版本主要跟Token计算相关

Logical channel可以指定逻辑通道，全局指定

Load length 可以指定下载cap文件时单条最大的长度

Timer 可以记录每条apdu的耗时

Log 运行Script或CAP下载时是否记录log

JCOP Remote Port可用来配置JCOP远程端口号，详细见9部分

Default config会将本页所有配置恢复成默认值

\*.xml配置



aid为安全域的AID，不填写默认是主安全域

ver为安全域密钥版本号

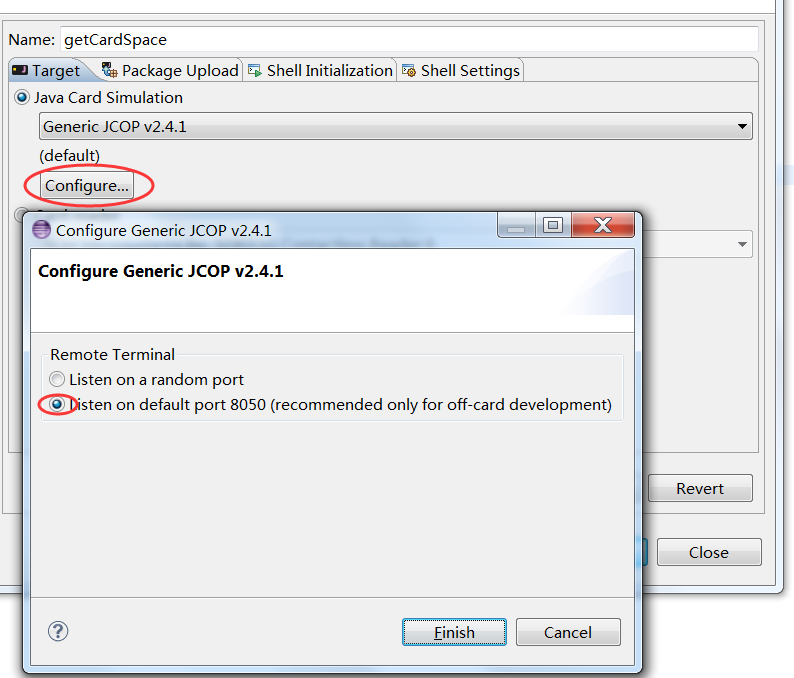
enc/mac/dek为安全域建立安全通道的一组密钥

当CFG栏的KMC不为No Diversify时kmc才起作用，此时enc/mac/dek不起作用

### JCOP

可以选择使用默认端口号或随机端口号：

1. 使用默认端口号8050

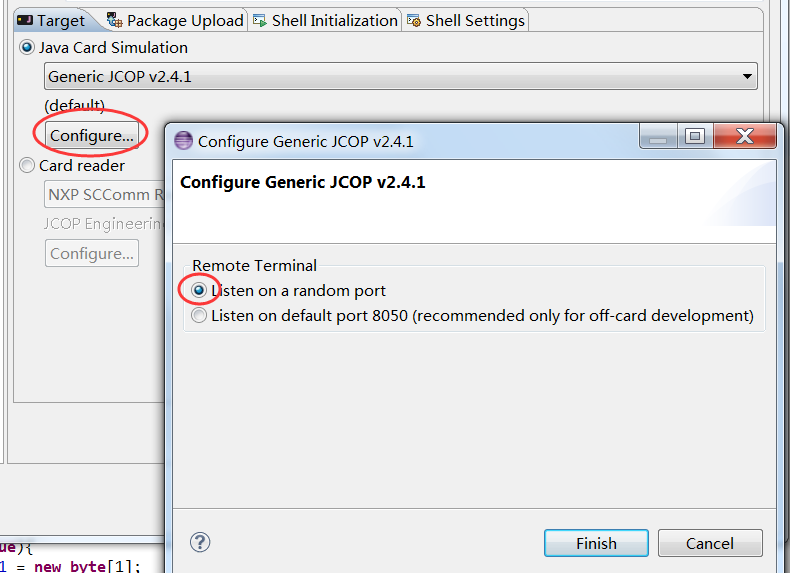


Eclipse Run/Debug时候配置端口为8050端口，如上图

使用SmartCardPlus连接JCOP前应当在JCOP Shell执行‘/close’指令,如下图

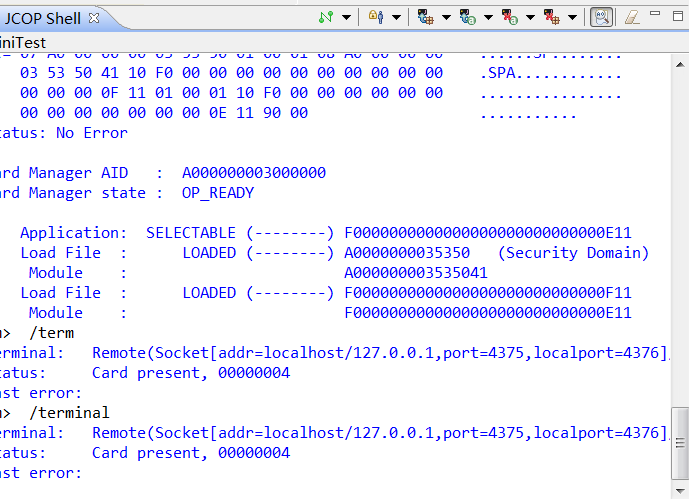


1. 使用随机端口号



Eclipse Run/Debug时候配置端口为随机端口，如上图

使用SmartCardPlus连接JCOP前应当在JCOP Shell执行‘/term’或‘/terminal’指令获取端口号,如下图（本图端口号为4375），同时配置SmartCard Plus Config选项的JCOP Remote Port。



JCOP Shell执行‘/close’指令

连接JCOP后2、3、4、5、7部分的操作均支持

## Ⅱ便捷功能

1. 在发送APDU时可以使用Enter键来发送
2. 可以把脚本、CAP直接拖到工具的路径栏
3. 选中View中Applet/Application/SecurityDomain时，可以批量删除多个应用或者安全域
4. 在VIEW中，鼠标左键选中某个AID后，再点鼠标右键可以复制该AID
5. 在VIEW中，鼠标移动到某个AID后，可以查看该AID的权限/生命周期
6. 使用上下方向键可以选择历史命令、脚本、CAP

## Ⅲ系统要求

1. 确保电脑已安装.netframework 4.0以上版本.
2. 已在windows xp、windows7、windows8、windows10测试通过..

## Ⅳ最新版本

SmartCard Plus及本文档的最新版本，请访问[SmartCard Plus](https://github.com/APDU/SmartCardPlus).

## Ⅴ注意事项

请勿删除软件目录下\*.xml，否则可能无法打开软件。

## Ⅵ历史记录

V2.9 2018.09.01 增加hmac、ecc、sha3算法、base64、base58、lua MACRO定义，lua api梳理等（旧版本的API不再支持）;

V2.8 2018.07.19 lua版本升级5.3.5;

V2.7 2018.06.28 增加SM1算法(ECB&CBC)，计算依赖算法卡;

V2.6 2017.09.15 增加luaAPI:rshift(int,int),lshift(int,int);

V2.5 2017.08.30 增加luaAPI:bitand(int,int),bitor(int,int),bitxor(int,int),xor(string,string);

V2.4 2017.08.04 UI调整，新增HASH算法，View新增Select功能

V2.3 2017.06.09 增加多读卡器的支持(最多3个)、增加AES算法、增加SM1加密数据

V2.2 2016.12.22 补充ALG.2说明,增加鸣谢

V2.1 2016.11.24 Script增加log说明，CFG增加Default Config说明

V2.0 2016.11.17 ALG2增加ID部分说明

V1.9 2016.11.07 更换UI截图，增加便捷功能部分

V1.8 2016.10.30 SCRIPT增加了txt格式脚本的关键字说明

V1.7 2016.10.27 VIEW增加Get STAT/Set STAT/Calc说明

V1.6 2016.10.26 SM2算法区分C=C1C2C3 与 C=C1C3C2，补充JCOP连接

V1.5 2016.09.12 增加XOR/ASCII功能，界面更新

V1.4 2016.09.08 增加DAP安全域的支持，增加PKCS1算法支持

V1.3 2016.09.02 UI调整

V1.2 2016.09.01 增加国密算法SM2/SM3/SM4

V1.1 2016.08.19 ALG中可以根据指定的P、Q产生RSA密钥

V1.0 2016.08.12 初始版本

## Ⅶ鸣谢

感谢PbocPub各位.