Phase5 Key Package导入指导文档

历史记录

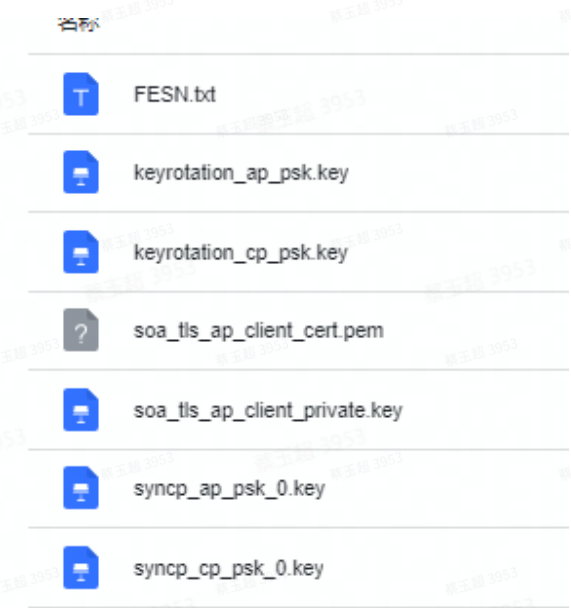
版本	日期	作者	内容
v0.1	2022-7-30	蔡玉超	初稿作成
v0.2	2022-8-4	蔡玉超	将TLS的Key放到configure分区
v0.3	2022-8-18	蔡玉超	将Syncp的Key放到configure分区

背景介绍

从08/04 R05开始，会默认Enable FNV soagateway TLS功能，默认系统起来后，在含有ECG、TCU的台架环境下，是无法进行SOA通信的，跟FNV相关的Feature都会不能正常使用，所以需要大家针对相应的环境申请对应的KEY Package。如果ECG、TCU是DEV的件，就申请DEV KEY Package，如果ECG、TCU是PRO的件，就需要申请PRO KEY Package。

Note： KEY Package可以找Ford的安全团队或者延锋进行申请。

KEY Package示例



DEV环境

步骤

1. 将 soa_tls_ap_client_cert.pem 和 soa_tls_ap_client_private.key 导入 `/configure/cert/`

   (PS：8月4日之前的R05版本导入的key路径：/vendor/etc/soa/gateway/config/)

```
CoffeeScript
1  adb root; adb remount
2  adb push soa_tls_ap_client_cert.pem /configure/cert/
3  adb push soa_tls_ap_client_private.key /configure/cert/
```

2. 将syncp_ap_psk_0.key导入 `/configure/cert/`

   （PS: 8月18日之后的R05版本导入的key路径：/vendor/etc/diagnostics/）

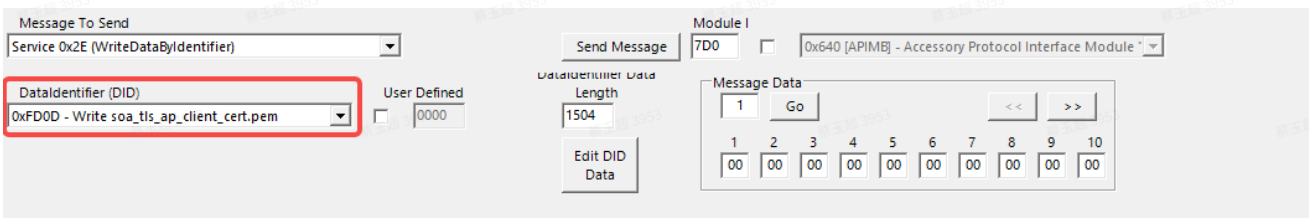
```
PowerShell
1  adb push syncp_ap_psk_0.key /configure/cert/
```

3. 重启台架

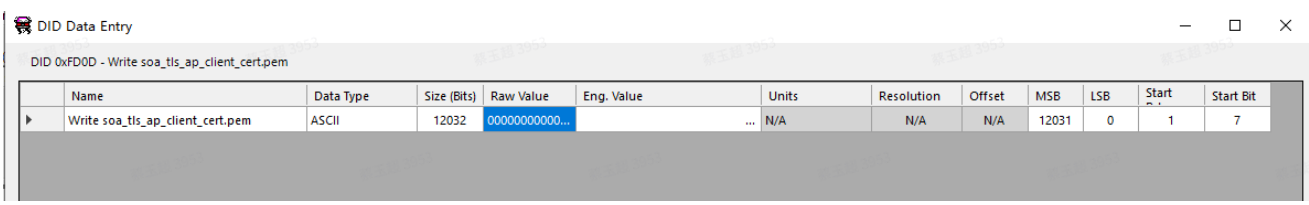
PRO环境

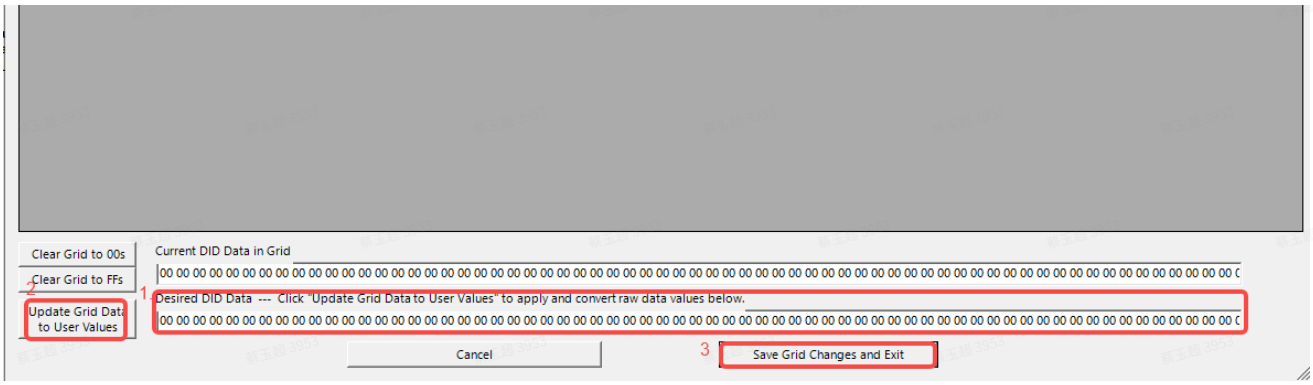
步骤

1. 将soa_tls_ap_client_cert.pem 和 soa_tls_ap_client_private.key文件内容转换成十六进制
2. 使用DET操作：发送10 60服务，再unlock，通过2E服务来写相关的key
   a. 使用与MCU版本对应的mdx和key文件
   b. 发送10 60，点击unlock
   c. 切换2E服务后，DataIdentifier处可以下拉选择对应key文件的DID

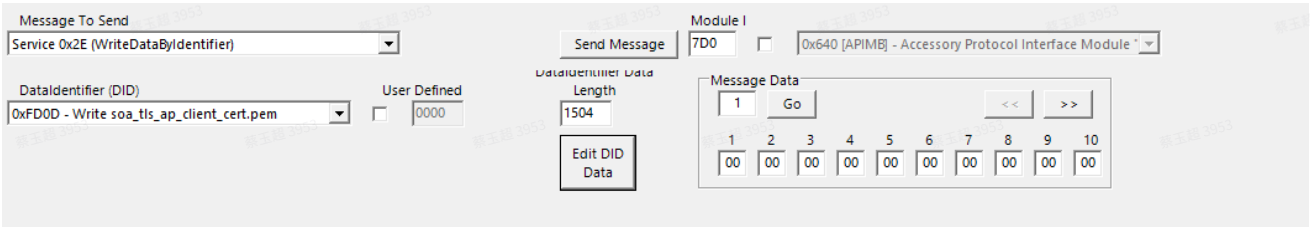


   d. 点击Edit DID Data，将第1步中的key的十六进制内容写入1框中，以“00”补齐字节；点击Update Grid Data to User Values按钮，若无报错，则点击Save；若显示字节数少于当前字节的错误，继续以“00”补齐字节





e. 点击send Message即可。



f. 其余key的刷写步骤同上。其DID值如下：

	A	B	C	D	E
1	Key Name	提供方	size(byte)	import/export	DID
2	syncp_ap_psk_0.key	FORD Secure package	50	import	FDC2
3			32	read	FDC3
4	keyrotation_ap_psk.key	FORD Secure package	50	import	FDC4
5			32	read	FDCB
6	syncp_cp_psk_0.key	FORD Secure package	50	import	FD09
7			32	read	FD0A
8	keyrotation_cp_psk.key	FORD Secure package	50	import	FD0B
9			32	read	FD0C
10	soa_tls_ap_client_cert.pem	FORD Secure package	1504	import	FD0D
11			32	read	FD0E
12	soa_tls_ap_client_private.key	FORD Secure package	1744	import	FD0F
13			32	read	FD19

功能确认

Key导入完成重启后，可通过以下功能进行确认KEY是否导入成功。

1. 在系统设置->常规设置->关于，可以看到TCU ESN信息。

2. 在不连接WiFi的情况下，可以正常刷出二维码信息。