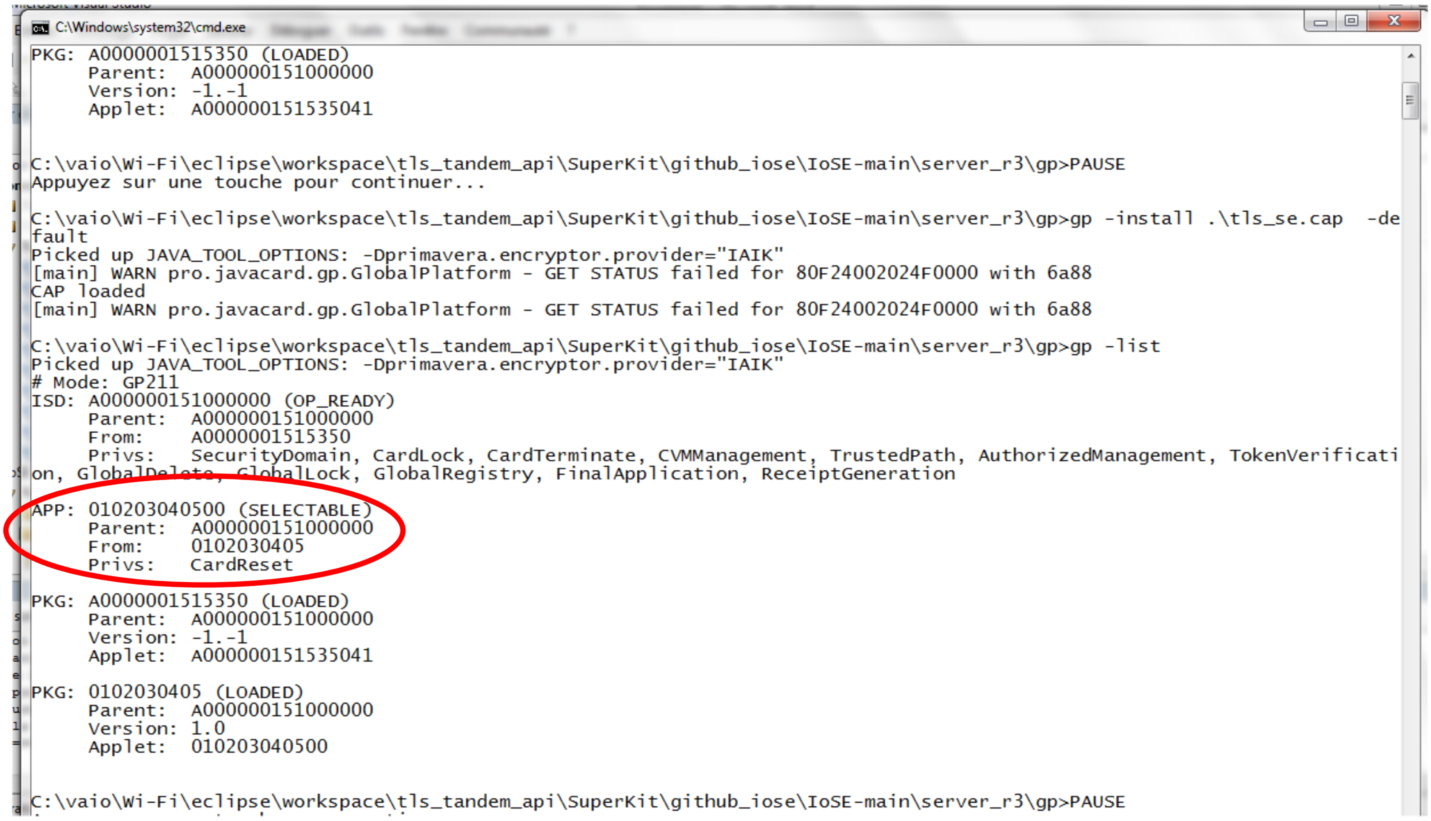
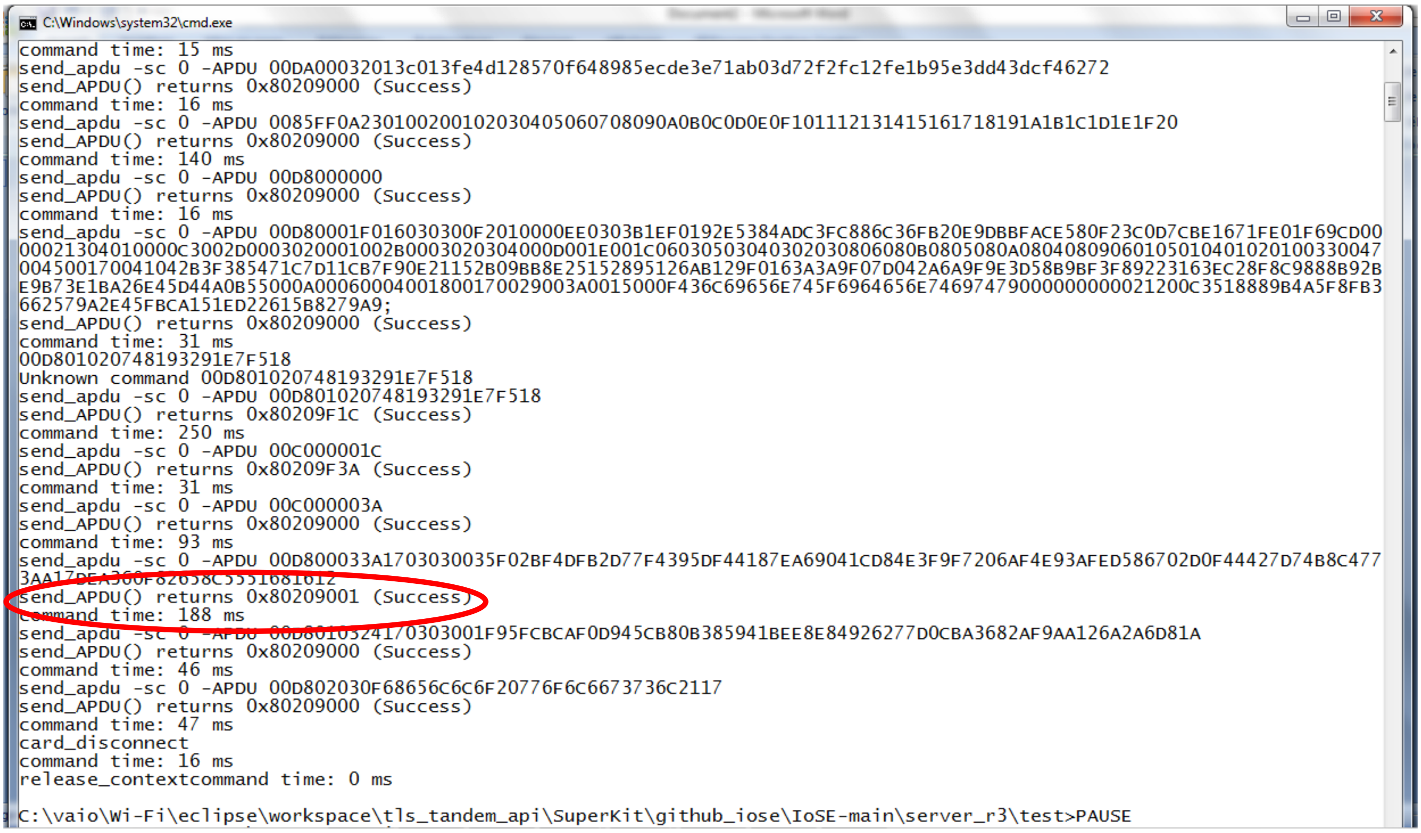
gp/load_tls_se_304.bat



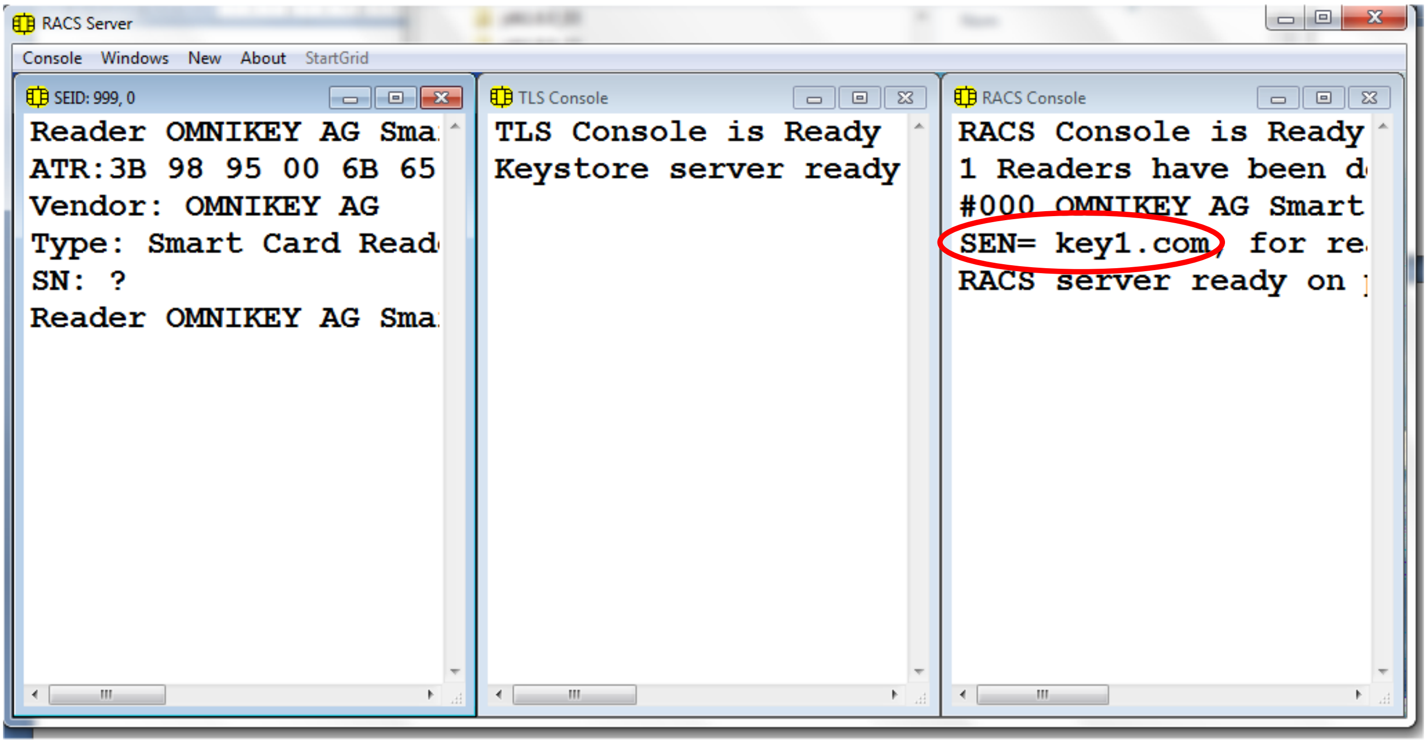
```
PKG: A0000001515350 (LOADED)
     Parent:  A000000151000000
     Version: -1.-1
     Applet:  A000000151535041


C:\vaio\Wi-Fi\eclipse\workspace\tls_tandem_api\SuperKit\github_iose\IoSE-main\server_r3\gp>PAUSE
Appuyez sur une touche pour continuer...

C:\vaio\Wi-Fi\eclipse\workspace\tls_tandem_api\SuperKit\github_iose\IoSE-main\server_r3\gp>gp -install .\tls_se.cap  -de
fault
Picked up JAVA_TOOL_OPTIONS: -Dprimavera.encryptor.provider="IAIK"
[main] WARN pro.javacard.gp.GlobalPlatform - GET STATUS failed for 80F24002024F0000 with 6a88
CAP loaded
[main] WARN pro.javacard.gp.GlobalPlatform - GET STATUS failed for 80F24002024F0000 with 6a88

C:\vaio\Wi-Fi\eclipse\workspace\tls_tandem_api\SuperKit\github_iose\IoSE-main\server_r3\gp>gp -list
Picked up JAVA_TOOL_OPTIONS: -Dprimavera.encryptor.provider="IAIK"
# Mode: GP211
ISD: A000000151000000 (OP_READY)
     Parent:  A000000151000000
     From:    A0000001515350
     Privs:   SecurityDomain, CardLock, CardTerminate, CVMManagement, TrustedPath, AuthorizedManagement, TokenVerificati
on, GlobalDelete, GlobalLock, GlobalRegistry, FinalApplication, ReceiptGeneration

APP: 010203040500 (SELECTABLE)
     Parent:  A000000151000000
     From:    0102030405
     Privs:   CardReset

PKG: A0000001515350 (LOADED)
     Parent:  A000000151000000
     Version: -1.-1
     Applet:  A000000151535041

PKG: 0102030405 (LOADED)
     Parent:  A000000151000000
     Version: 1.0
     Applet:  010203040500


C:\vaio\Wi-Fi\eclipse\workspace\tls_tandem_api\SuperKit\github_iose\IoSE-main\server_r3\gp>PAUSE
```

test/test.bat



```
command time: 15 ms
send_apdu -sc 0 -APDU 00DA00032013c013fe4d128570f648985ecde3e71ab03d72f2fc12fe1b95e3dd43dcf46272
send_APDU() returns 0x80209000 (Success)
command time: 16 ms
send_apdu -sc 0 -APDU 0085FF0A2301002001020304050607080 90A0B0C0D0E0F101112131415161718191A1B1C1D1E1F20
send_APDU() returns 0x80209000 (Success)
command time: 140 ms
send_apdu -sc 0 -APDU 00D8000000
send_APDU() returns 0x80209000 (Success)
command time: 16 ms
send_apdu -sc 0 -APDU 00D80001F016030300F2010000EE0303B1EF0192E5384ADC3FC886C36FB20E9DBBFACE580F23C0D7CBE1671FE01F69CD00
00021304010000C3002D0003020001002B0003020304000D001E001C06030503040302030806080B0805080A08040809060105010401020100330047
004500170041042B3F385471C7D11CB7F90E21152B09BB8E25152895126AB129F0163A3A9F07D042A6A9F9E3D58B9BF3F89223163EC28F8C9888B92B
E9B73E1BA26E45D44A0B55000A00060004001800170029003A0015000F436C69656E745F6964656E74697479000000000021200C3518889B4A5F8FB3
662579A2E45FBCA151ED22615B8279A9;
send_APDU() returns 0x80209000 (Success)
command time: 31 ms
00D801020748193291E7F518
Unknown command 00D801020748193291E7F518
send_apdu -sc 0 -APDU 00D801020748193291E7F518
send_APDU() returns 0x80209F1C (Success)
command time: 250 ms
send_apdu -sc 0 -APDU 00C000001C
send_APDU() returns 0x80209F3A (Success)
command time: 31 ms
send_apdu -sc 0 -APDU 00C000003A
send_APDU() returns 0x80209000 (Success)
command time: 93 ms
send_apdu -sc 0 -APDU 00D800033A1703030035F02BF4DFB2D77F4395DF44187EA69041CD84E3F9F7206AF4E93AFED586702D0F44427D74B8C477
3AA17DEA360F82658C5551681612
send_APDU() returns 0x80209001 (Success)
command time: 188 ms
send_apdu -sc 0 -APDU 00D8010324170303001F95FCBCAF0D945CB80B385941BEE8E84926277D0CBA3682AF9AA126A2A6D81A
send_APDU() returns 0x80209000 (Success)
command time: 46 ms
send_apdu -sc 0 -APDU 00D802030F68656C6C6F20776F6C6673736C2117
send_APDU() returns 0x80209000 (Success)
command time: 47 ms
card_disconnect
command time: 16 ms
release_contextcommand time: 0 ms

C:\vaio\Wi-Fi\eclipse\workspace\tls_tandem_api\SuperKit\github_iose\IoSE-main\server_r3\test>PAUSE
```

IOSE.exe

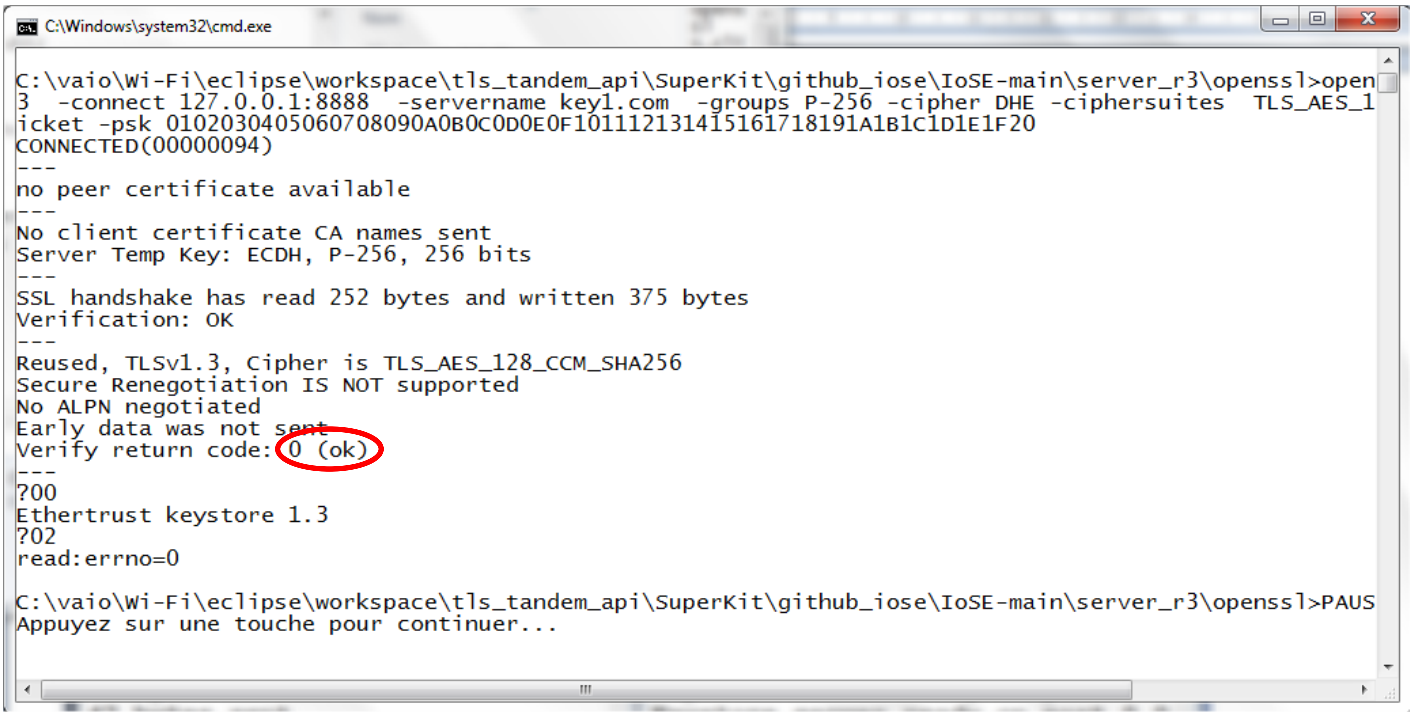


```
Reader OMNIKEY AG Sma
ATR:3B 98 95 00 6B 65
Vendor: OMNIKEY AG
Type: Smart Card Read
SN: ?
Reader OMNIKEY AG Sma
```

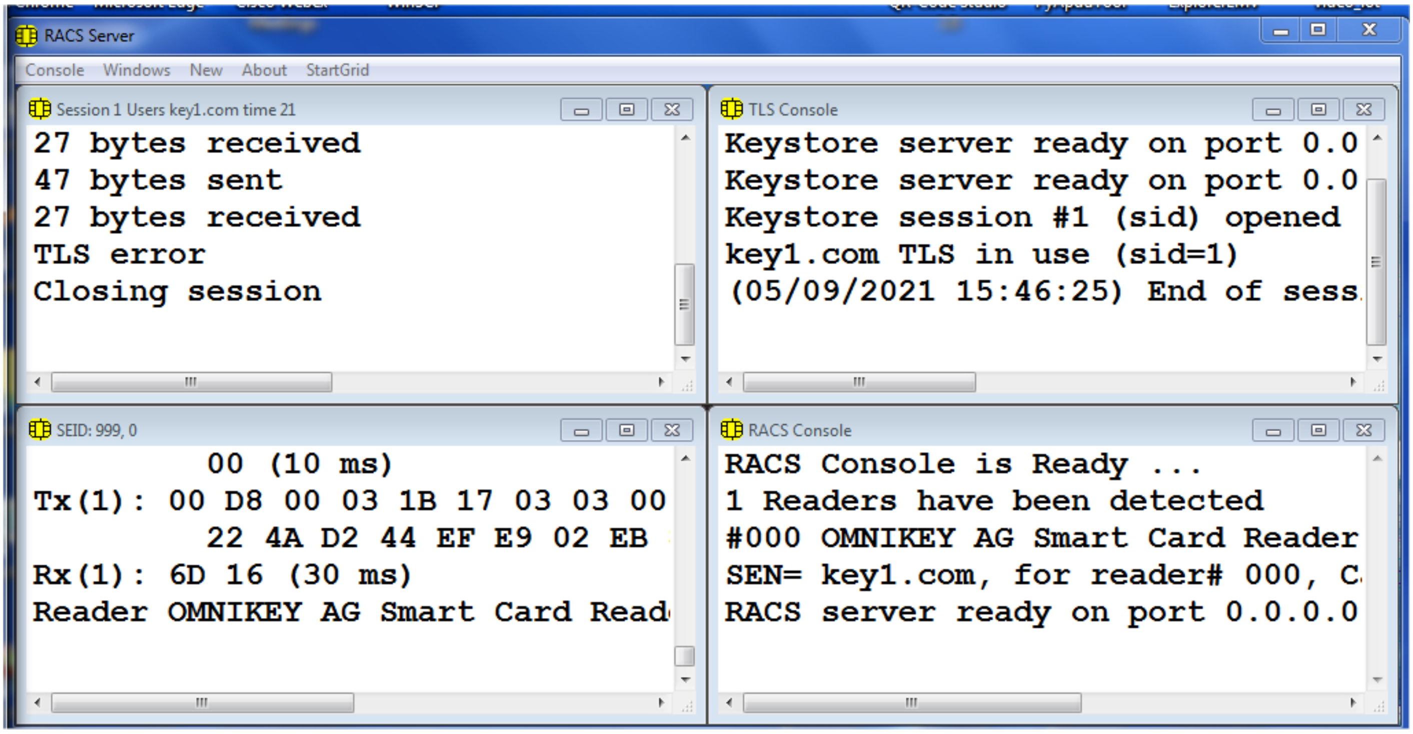
```
TLS Console is Ready
Keystore server ready
```

```
RACS Console is Ready
1 Readers have been d
#000 OMNIKEY AG Smart
SEN= key1.com, for re
RACS server ready on
```

openssl/OPENSSL_TLS_SE_LOCAL_8888



```
C:\vaio\Wi-Fi\eclipse\workspace\tls_tandem_api\SuperKit\github_iose\IoSE-main\server_r3\openssl>open
3  -connect 127.0.0.1:8888  -servername key1.com  -groups P-256 -cipher DHE -ciphersuites  TLS_AES_1
icket -psk 0102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F20
CONNECTED(00000094)
---
no peer certificate available
---
No client certificate CA names sent
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 252 bytes and written 375 bytes
Verification: OK
---
Reused, TLSv1.3, Cipher is TLS_AES_128_CCM_SHA256
Secure Renegotiation IS NOT supported
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
?00
Ethertrust keystore 1.3
?02
read:errno=0

C:\vaio\Wi-Fi\eclipse\workspace\tls_tandem_api\SuperKit\github_iose\IoSE-main\server_r3\openssl>PAUS
Appuyez sur une touche pour continuer...
```



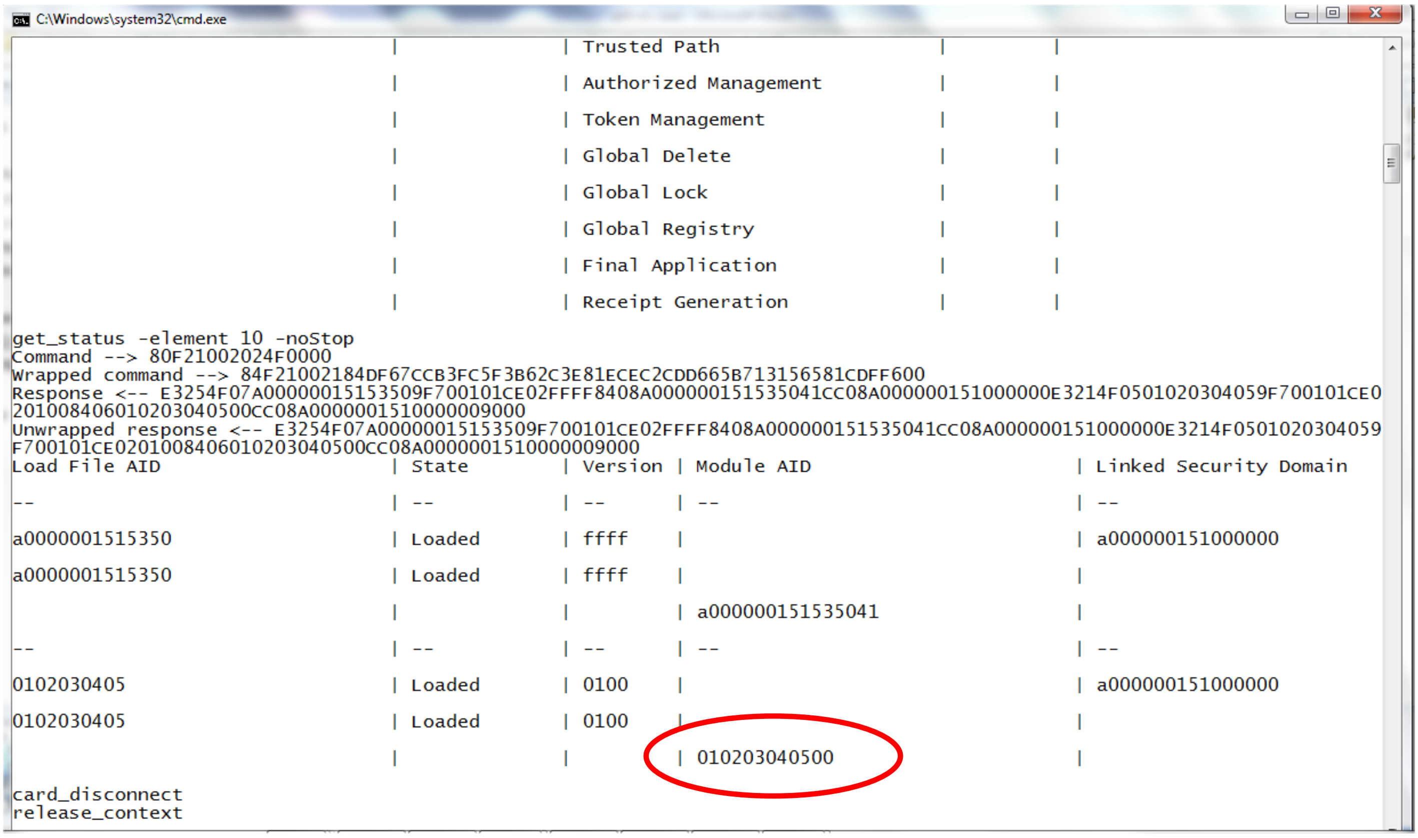
```
27 bytes received
47 bytes sent
27 bytes received
TLS error
Closing session
```

```
Keystore server ready on port 0.0
Keystore server ready on port 0.0
Keystore session #1 (sid) opened
key1.com TLS in use (sid=1)
(05/09/2021 15:46:25) End of sess
```

```
        00 (10 ms)
Tx(1): 00 D8 00 03 1B 17 03 03 00
        22 4A D2 44 EF E9 02 EB
Rx(1): 6D 16 (30 ms)
Reader OMNIKEY AG Smart Card Read
```

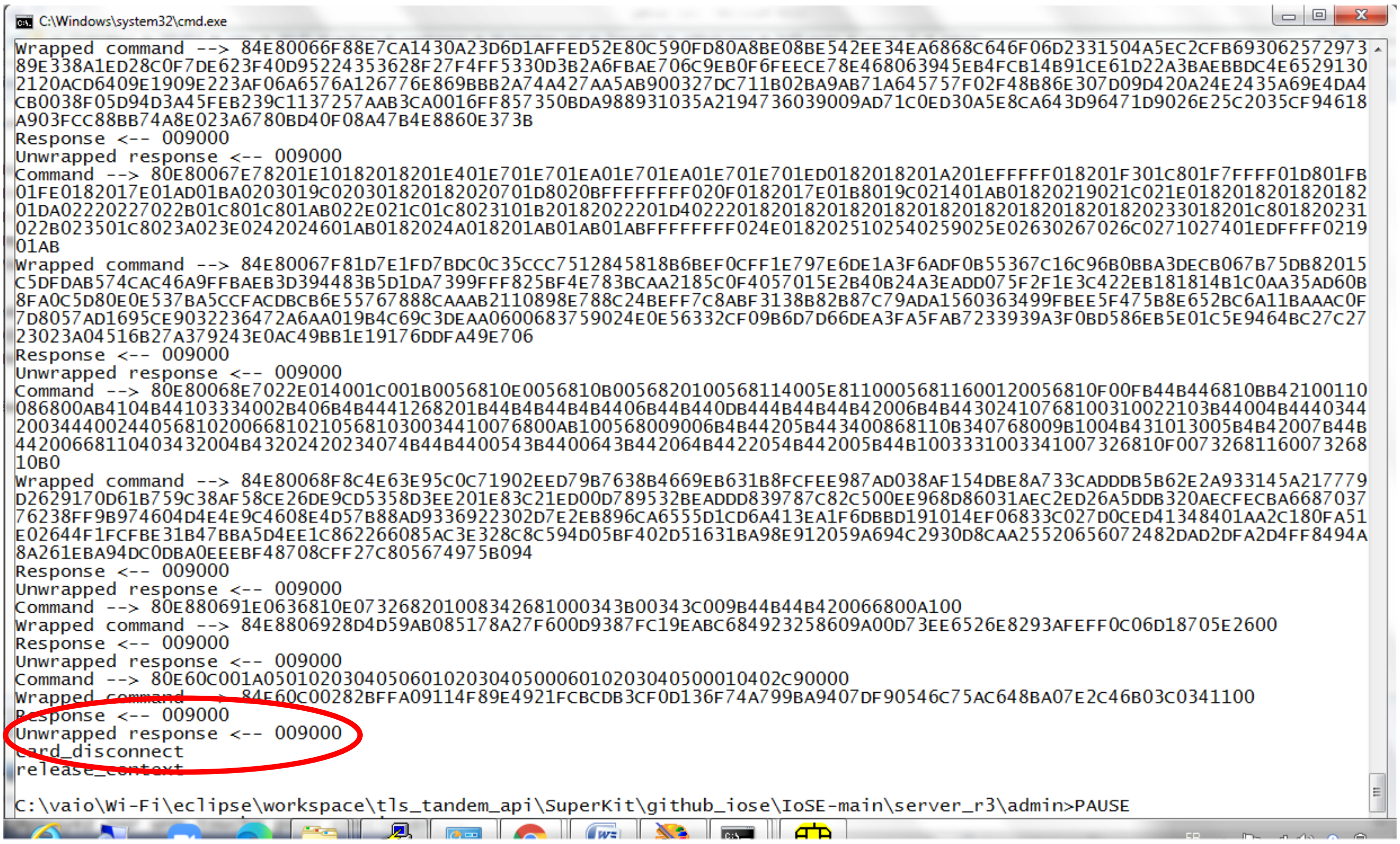
```
RACS Console is Ready ...
1 Readers have been detected
#000 OMNIKEY AG Smart Card Reader
SEN= key1.com, for reader# 000, C
RACS server ready on port 0.0.0.0
```

admin/list_SCP03.bat



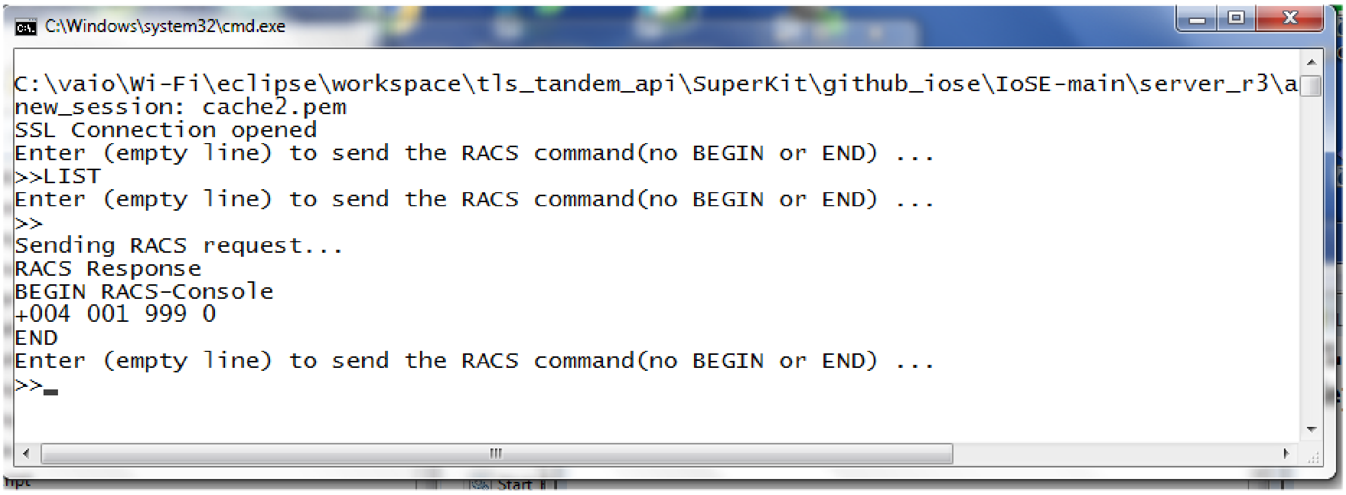
```
                                 |              | Trusted Path                   |         |
                                 |              | Authorized Management          |         |
                                 |              | Token Management               |         |
                                 |              | Global Delete                  |         |
                                 |              | Global Lock                    |         |
                                 |              | Global Registry                |         |
                                 |              | Final Application              |         |
                                 |              | Receipt Generation             |         |

get_status -element 10 -noStop
Command --> 80F21002024F0000
Wrapped command --> 84F21002184DF67CCB3FC5F3B62C3E81ECEC2CDD665B713156581CDFF600
Response <-- E3254F07A00000015153509F700101CE02FFFF8408A000000151535041CC08A000000151000000E3214F0501020304059F700101CE0
201008406010203040500CC08A00000015100000009000
Unwrapped response <-- E3254F07A00000015153509F700101CE02FFFF8408A000000151535041CC08A000000151000000E3214F0501020304059
F700101CE0201008406010203040500CC08A00000015100000009000
Load File AID                    | State        | Version | Module AID                     | Linked Security Domain
--                               | --           | --      | --                             | --
a0000001515350                   | Loaded       | ffff    |                                | a000000151000000
a0000001515350                   | Loaded       | ffff    |                                |
                                 |              |         | a000000151535041               |
--                               | --           | --      | --                             | --
0102030405                       | Loaded       | 0100    |                                | a000000151000000
0102030405                       | Loaded       | 0100    |                                |
                                 |              |         | 010203040500                   |
card_disconnect
release_context
```

admin/helloInstallSCP03

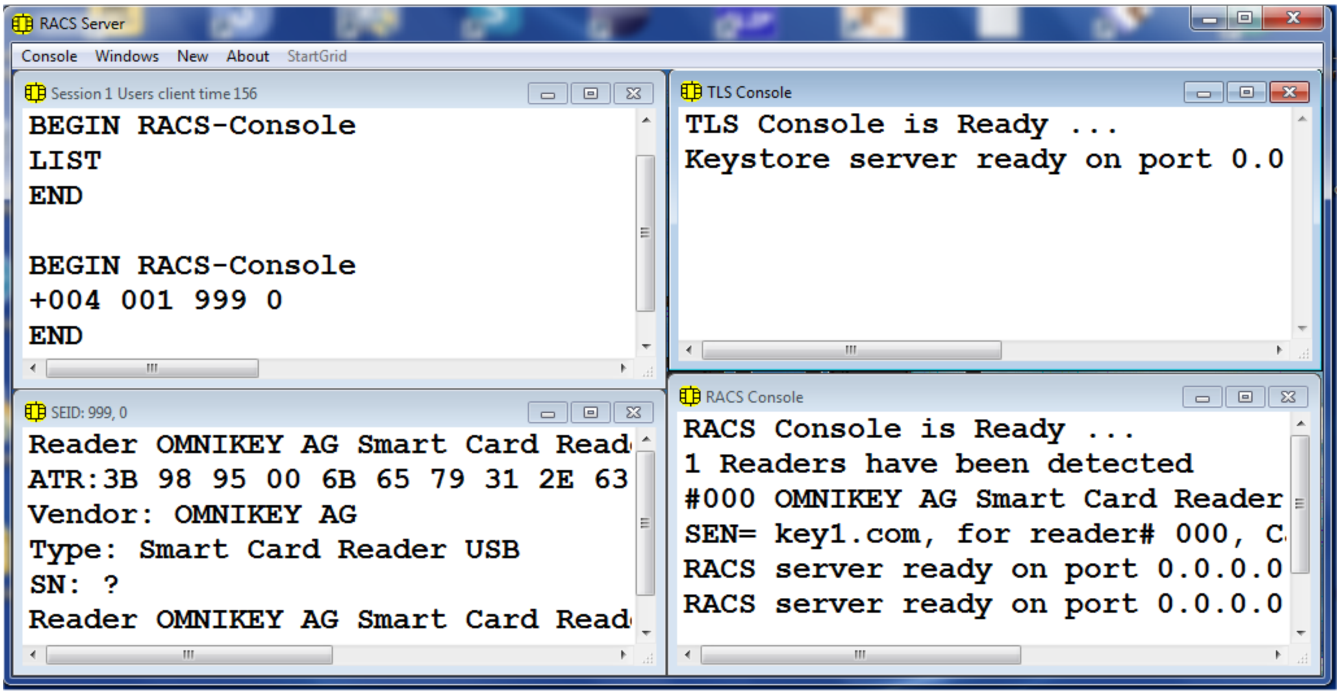


```
Wrapped command --> 84E80066F88E7CA1430A23D6D1AFFED52E80C590FD80A8BE08BE542EE34EA6868C646F06D2331504A5EC2CFB693062572973
89E338A1ED28C0F7DE623F40D95224353628F27F4FF5330D3B2A6FBAE706C9EB0F6FEECE78E468063945EB4FCB14B91CE61D22A3BAEBBDC4E6529130
2120ACD6409E1909E223AF06A6576A126776E869BBB2A74A427AA5AB900327DC711B02BA9AB71A645757F02F48B86E307D09D420A24E2435A69E4DA4
CB0038F05D94D3A45FEB239C1137257AAB3CA0016FF857350BDA988931035A219473603900 9AD71C0ED30A5E8CA643D96471D9026E25C2035CF94618
A903FCC88BB74A8E023A6780BD40F08A47B4E8860E373B
Response <-- 009000
Unwrapped response <-- 009000
Command --> 80E80067E78201E10182018201E401E701E701EA01E701EA01E701E701ED0182018201A201EFFFFF018201F301C801F7FFFF01D801FB
01FE0182017E01AD01BA0203019C0203018201820207 01D8020BFFFFFFFF020F0182017E01B8019C021401AB01820219021C021E0182018201820182
01DA02220227022B01C801C801AB022E021C01C8023101B20182022201D402220182018201820182018201820182018201820233018201C801820231
022B023501C8023A023E0242024601AB0182024A018201AB01AB01ABFFFFFFFF024E0182025102540259025E02630267026C0271027401EDFFFF0219
01AB
Wrapped command --> 84E80067F81D7E1FD7BDC0C35CCC7512845818B6BEF0CFF1E797E6DE1A3F6ADF0B55367C16C96B0BBA3DECB067B75DB82015
C5DFDAB574CAC46A9FFBAEB3D394483B5D1DA7399FFF825BF4E783BCAA2185C0F4057015E2B40B24A3EADD075F2F1E3C422EB181814B1C0AA35AD60B
8FA0C5D80E0E537BA5CCFACDBCB6E55767888CAAAB2110898E788C24BEFF7C8ABF3138B82B87C79ADA1560363499FBEE5F475B8E652BC6A11BAAAC0F
7D8057AD1695CE9032236472A6AA019B4C69C3DEAA0600683759024E0E56332CF09B6D7D66DEA3FA5FAB7233939A3F0BD586EB5E01C5E9464BC27C27
23023A04516B27A379243E0AC49BB1E19176DDFA49E706
Response <-- 009000
Unwrapped response <-- 009000
Command --> 80E80068E7022E014001C001B0056810E0056810B0056820100568114005E81100056811600120056810F00FB44B446810BB42100110
086800AB4104B44103334002B406B4B4441268201B44B4B44B4B4406B44B440DB444B44B44B42006B4B44302410768100310022103B44004B4440344
200344400244056810200668102105681030034410076800AB100568009006B4B44205B443400868110B340768009B1004B431013005B4B42007B44B
44200668110403432004B43202420234074B44B4400543B4400643B442064B4422054B442005B44B1003331003341007326810F00732681160073268
10B0
Wrapped command --> 84E80068F8C4E63E95C0C71902EED79B7638B4669EB631B8FCFEE987AD038AF154DBE8A733CADDDB5B62E2A933145A217779
D2629170D61B759C38AF58CE26DE9CD5358D3EE201E83C21ED00D789532BEADDD839787C82C500EE968D86031AEC2ED26A5DDB320AECFECBA6687037
76238FF9B974604D4E4E9C4608E4D57B88AD9336922302D7E2EB896CA6555D1CD6A413EA1F6DBBD191014EF06833C027D0CED41348401AA2C180FA51
E02644F1FCFBE31B47BBA5D4EE1C862266085AC3E328C8C594D05BF402D51631BA98E912059A694C2930D8CAA25520656072482DAD2DFA2D4FF8494A
8A261EBA94DC0DBA0EEEBF48708CFF27C805674975B094
Response <-- 009000
Unwrapped response <-- 009000
Command --> 80E880691E0636810E07326820100834268100034 3B00343C009B44B44B420066800A100
Wrapped command --> 84E8806928D4D59AB085178A27F600D9387FC19EABC684923258609A00D73EE6526E8293AFEFF0C06D18705E2600
Response <-- 009000
Unwrapped response <-- 009000
Command --> 80E60C001A0501020304050601020304050006010203040500010402C90000
Wrapped command --> 84E60C00282BFFA09114F89E4921FCBCDB3CF0D136F74A799BA9407DF90546C75AC648BA07E2C46B03C0341100
Response <-- 009000
Unwrapped response <-- 009000
card_disconnect
release_context

C:\vaio\Wi-Fi\eclipse\workspace\tls_tandem_api\SuperKit\github_iose\IoSE-main\server_r3\admin>PAUSE
```

admin/Start_RACS_Console_Local.bat



```
C:\vaio\Wi-Fi\eclipse\workspace\tls_tandem_api\SuperKit\github_iose\IoSE-main\server_r3\a
new_session: cache2.pem
SSL Connection opened
Enter (empty line) to send the RACS command(no BEGIN or END) ...
>>LIST
Enter (empty line) to send the RACS command(no BEGIN or END) ...
>>
Sending RACS request...
RACS Response
BEGIN RACS-Console
+004 001 999 0
END
Enter (empty line) to send the RACS command(no BEGIN or END) ...
>>_
```



```
BEGIN RACS-Console
LIST
END

BEGIN RACS-Console
+004 001 999 0
END
```

```
TLS Console is Ready ...
Keystore server ready on port 0.0
```

```
Reader OMNIKEY AG Smart Card Read
ATR:3B 98 95 00 6B 65 79 31 2E 63
Vendor: OMNIKEY AG
Type: Smart Card Reader USB
SN: ?
Reader OMNIKEY AG Smart Card Read
```

```
RACS Console is Ready ...
1 Readers have been detected
#000 OMNIKEY AG Smart Card Reader
SEN= key1.com, for reader# 000, C
RACS server ready on port 0.0.0.0
RACS server ready on port 0.0.0.0
```