z/TPF SSL Socket Driver User's Guide

1.0 Introduction

This driver is used to test the basic and expanded functionality of the SSL code in TPF. Its function is determined by an input file provided to the program. This input file will contain all the information which is variable, such as IP address, port, cipher, certificate file etc. Although this driver is different from the socket driver, they are started via the same start up program (QXYA).

2.0 Syntax Information

I. Syntax Diagram:

```
>>|-ZTEST-|---|-SOCK-SSL-|-SERVER-|-|----|-file-|-----|-|-|--|------------|
          |-i-|           |-CLIENT-| |SESS|      |-num-| |d|  |-RIP-x.x.x.x|
                          |-SERVER2|
                          |-CLIENT2|
```

Where:

PARAMETER	DESCRIPTION
i	This is an optional variable that indicates the specific I-stream in which the driver of the specific test case will be run. If **i** is not specified, the test case(s) will be executed on the I-stream on which the command is entered. If * is specified, the test case(s) will be invoked on all currently defined and available I streams.
SOCK	This is a required keyword that specifies that the SOCK driver is to be run.
SSL	This is a required keyword that specifies that the SSL driver is to be run.
SERVER	This keyword specifies that the driver is to be run as a server. This option must be used in conjunction with the CLIENT option for the remote partner
SERVER2	This keyword specifies that the driver is to be run as a server running the performance option for starting SSL sessions. This option does not transfer any data (fields in the config file are ignored) and simply starts the session then ends it. This option must be used in conjunction with the CLIENT2 option. This option is only valid for configuration files that specify to use shared SSL.
CLIENT	This keyword specifies that the driver is to be run as a client. This option must be used in conjunction with the SERVER option for the remote partner.
CLIENT2	This keyword specifies that the driver is to be run as a client running the performance option for starting SSL sessions. This option does not transfer any data (fields in the config file are ignored) and simply starts the session then ends it. This option must be used in conjunction with the SERVER2 option. This option is only valid for configuration files that specify to use shared SSL.

file	This is the name, with full path, of the parameter file to be used. The name and path may NOT exceed 15 characters. See Appendix A for sample input files.
num	This is the number of clients to be started. This parameter is only valid if the CLIENT keyword is used.
sess	This option is only valid with the CLIENT2 option. It specifies how many sessions to start for each client specified (num) on the command.
d	This parameter specifies the time interval to wait (in seconds) between starting the SSL clients. For example, if on the CLIENT command you specified to start 10 clients, this paramter specifies the time interval to wait in between starting each. This option is only valid for the CLIENT parameter.
RIP	This parameter allows you to override the value in the SSL configuration file as to whom to connect to. This option is primarily used when using the predefined keys and certificates. This option is only valid when CLIENT or CLIENT2 is specified.

I. Sample Invocations

- ZTEST SOCK SSL SERVER /SERV *This command will start a server with /SERV as the input file.*
- ZTEST SOCK SSL CLIENT /CLI 1 *This command will start 1 client with /CLI as the input file.*
- ZTEST SOCK SSL SERVER2 /SERV *This command will start the performance server with the /SERV as the input file.*
- ZTEST SOCK SSL CLIENT2 100 /CLI 10 *This command will start 10 clients all starting 100 sessions with the /CLI as the input file.*

3.0 Driver Messages

This driver has a number of error messages which are self explanatory.

Appendix A : Input files

The input file is simply a flat file with some keywords in no specific order. Some of the keywords are mandatory and some are optional. All keywords must be in upper case, but the parameters associated with a keyword do not have to be upper case.

Mandatory keywords:

Keyword	**Description**
IP-xxx.xxx.xxx.xxx	The ip address of the server.
PORT-xxxx	The port of the server.
CIPHER-xxx,yyy,zzzz	The list of all the ciphers to be used by the driver. Valid ciphers are: • RC4-MD5 • RC4-SHA • RC2-CBC-MD5 • DES-CBC-SHA • DES-CBC-MD5 • DES-CBC3-SHA • DES-CBC3-MD5 • AES128-SHA • AES256-SHA • NULL-MD5 • NULL-SHA
VERSION-xxx	The SSL version to be used by the driver. Valid versions are: • V20 - SSL version 2 • V30 - SSL version 3 • V23 - SSL version 2-3 • TLS10 - TLS version 1.0
CERT-xxxxx	The certificate file the driver will use. It must contain the full path, and it is case sensitive.
KEY-xxxx	The key file the driver will use. It must contain the full path, and it is case sensitive.
ROLE-xxxx	Determines the drivers role. The role on the server should be the opposite of the role on the client, unless it is BOUNCE. Valid roles are: • SEND • READ • BOUNCE
MNUM-xxx	The number of messages to be send/read. This number should be the same in both the server and the client.
MSIZE-xxx	The size of the message to be sent; it has a maximum size of 100,000. This number should be the same in both the server and the client.

The optional parameters are:

Keyword	Description
CAFILE-xxxx	The file that contains the certificates of the trusted CA¡¯s. Full path must be given. Using this keyword will enable peer verification
CADIR-xxxx	The directory that contains the certificate of the trusted CA¡¯s. Full path must be given. Using this keyword will enable peer verification
CHAIN	This indicates that the certificate indicated in the CERT keyword is a chain certificate.
KEYPASS-xxxx	The passworof the Key file. Omission of this keyword means that the key does not require a password.
CRL-xxxx	The file that contains the certificate revocation list (CRL). Full path must be given.
SHARED	This indicates that a shared session will be used for the driver.
CTXNAME-xxxx	This gives the name to be used when creating the CTX. If it is omitted and the SHARED keyword is specified it is defaulted to NULL.
AOR	This keyword indicates that all reads will be done through a call to the SSL_aor function.
COUNT-xxx	This specifies the number of ECB's to be created to send through one session. The Count keyword in the client won't cause more ECB's to be created, but it will change the way the messages are processed when they are received. This keyword is only valid when the SHARED keyword is used.

Sample server input file content:

```
IP-9.117.249.71
PORT-1000
VERSION-V23
CIPHER-RC4-MD5,RC4-SHA,DES-CBC-MD5,DES-CBC3-MD5,DES-CBC-SHA,DES-CBC3-SHA
ROLE-SEND
MNUM-10000
MSIZE-200
CERT-/certs/visacert.pem
KEY-/certs/visakey.pem
CAFILE-/certs/visaca.pem
SHARED
CTXNAME-EVERYONE
```

Sample client input file content:

```
IP-9.117.249.71
PORT-1000
VERSION-V23
CIPHER-RC4-MD5,RC4-SHA,DES-CBC-MD5,DES-CBC3-MD5,DES-CBC-SHA,DES-CBC3-SHA
CERT-/certs/visacert.pem
KEY-/certs/visakey.pem
KEYPAS-aname
CAFILE-/certs/visaca.pem
ROLE-READ
MNUM-10000
MSIZE-200
SHARED
AOR
```