

OpenSSL in 21CS VSEⁿ

Preparation & Configuration

Shahin Ram Krishna

shahin.krishna@21cs.com



21CS

Agenda

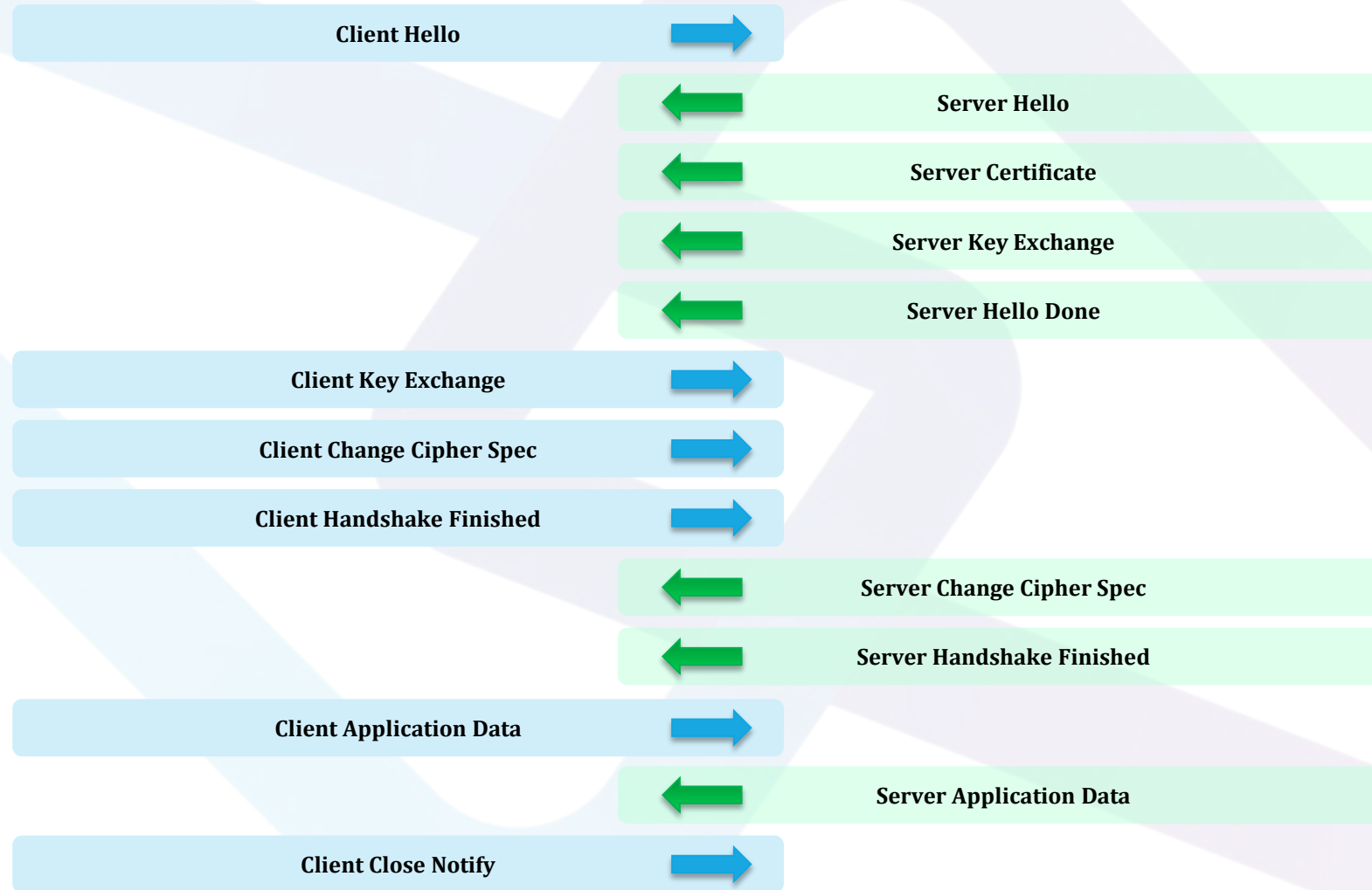


- What is OpenSSL and TLS?
- Prerequisites and Optional
- Multiplexer: EDCTCPMC.PHASE
- OpenSSL with TCP/IP for VSEⁿ by CSI
- OpenSSL with IPv6/VSEⁿ IPv4 TCP/IP by BSI

What is OpenSSL and TLS?

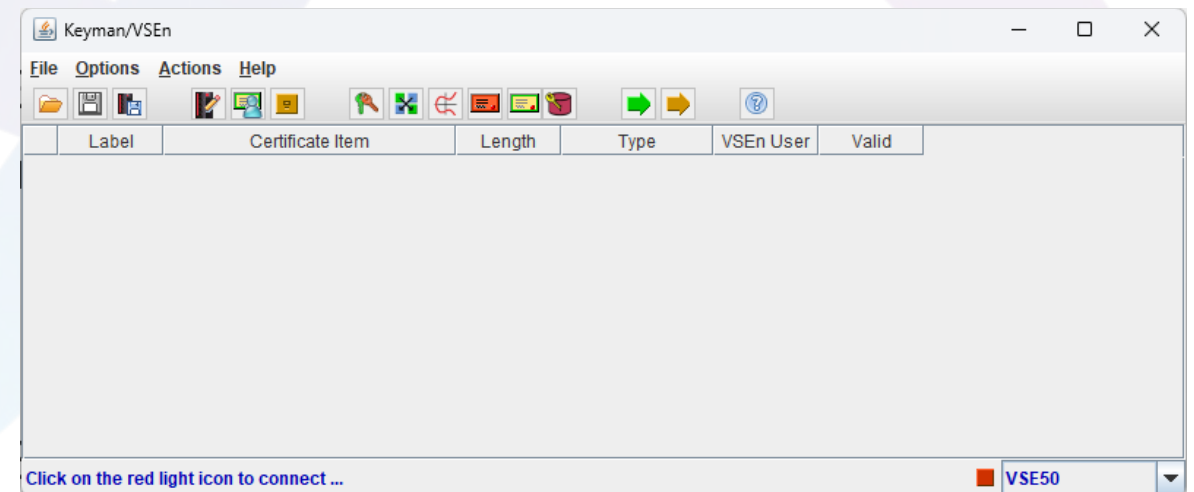
- OpenSSL is a robust, commercial-grade, full-featured Open-Source Toolkit for the TLS (formerly SSL), DTLS and QUIC protocols.
 - Creation of Key Parameters
 - Creation of certificates
 - Encryption and decryption
 - and more ...

Overview of TLS Communication



Prerequisites / Optional

- Running VSEn 6.3 or newer
- With functional TCP/IP Stack
 - Either: 21CS TCP/IP for VSEn (“CSI”), 21CS IPv6/VSE (“BSI), or 21CS LFP for VSEn
 - Functional FTP capability
 - Functional TELNET capability
- Certificate
 - X.509
- Optional Certificate Generation
 - With Keyman support





EDCTCPMC.PHASE



- Multiplexer
- Allows you to use standard commands for TCP/IP operations, no matter the stack
- Skeleton ICCF.62(EDCTCPMC)
- Provided in Library
- Add SSLPHASE='IJBSSLE'

```
+
+
+   Using sysid 0 for TCP/IP and SSL from CSI (default value):
+   EDCTCPME SYSID='00',PHASE='$EDCTCPV'
+   EDCTCPME SYSID='00',PHASE='$EDCTCPV',SSLPHASE='IJBSSLE'
+
+
+   Using sysid 1 for TCP/IP and SSL from BSI (IPv4 or IPv6):
+   EDCTCPME SYSID='01',PHASE='BSTTTTCP6'
+   EDCTCPME SYSID='01',PHASE='BSTTTTCP6',SSLPHASE='IJBSSLE'
+
+
+   Using sysid 2 for TCP/IP via LFP and SSL via OpenSSL:
+   EDCTCPME SYSID='02',PHASE='IJBLEFPLE',SSLPHASE='IJBSSLE'
+
```

- Developed by CSI International
- Provides IPv4 support
- Provides SSL Engine CSINTSSL
- Also allows to use VSEn OpenSSL

TCP/IP Command

```
OPENSSL ON
```

JCL SETPARAM

```
// SETPARAM CRYSERV='OPENSSL'
```

21CS TCP/IP for VSEⁿ: Define FTPS Daemon



NON-SSL FTP Daemon

```
DEFINE FTP,ID=FTP50PORT,PORT=21,COUNT=2,DYNFILES=YES
```

SSL Enabled FTP Daemon

```
DEFINE FTP,ID=FTPSSL, COUNT=2,DYNFILES=YESPORT=990,  
SSL=YES,SSLKEY=CRYPTO.KEYRING.VSE50,SSLVERSION=TLS12
```

Non-SSL Telnet Daemon

```
DEFINE TELNETD,  
    ID=TNNSSL,  
    TERMNAME=TELNLU,  
    TARGET=DBDCCICS,  
    PORT=23,  
    COUNT=2,  
    POOL=YES
```

SSL Enabled Telnet Daemon

```
DEFINE TELNETD,  
    ID=TNNSSL,  
    TERMNAME=TELNLU,  
    TARGET=DBDCCICS,  
    PORT=992,  
    COUNT=2,  
    POOL=YES,  
    SSL=YES,  
    SSLLIBRARY=CRYPTO,  
    SSLSUBLIBRARY=KEYRING,  
    SSLMEMBER=VSE50,  
    SSLVERSION=TLS13
```



21CS IPv6/VSE



- Provides IPv4 and IPv6 support
- Developed by Barnard Software, Inc.
- TCP/IP Applications run in their “own” stack
- OpenSSL is an addition to the TCP/IP application
 - The application needs more space (partition storage)

```
F4 , FEC , J4 ,          INACTIVE ,
F5 , FEC , H5 ,    FTPNSRVR , 00340 , 5
F6 , FEC , M6 ,          INACTIVE ,
F7 , FEC , N7 ,    TCPIP01  , 00339 , 7
F8 , FEC , P8 ,          INACTIVE ,
```

Non-SSL FTP Server

```
// LIBDEF *,SEARCH=(PRD2.CONFIG,PRD2.TCPIPB)
// EXEC BSTTFTPS,SIZE=BSTTFTPS
ID 01
*
OPEN 192.168.22.150 21
*
SMNT LIBRARY PRD2
*
ATTACH SERVER-1
ATTACH SERVER-2
*
/*
```

SSL Enabled FTP Server

```
// LIBDEF *,SEARCH=(PRD2.CONFIG,PRD2.TCPIPB)
// EXEC BSTTFTPS,SIZE=BSTTFTPS
ID 01
*
XTLS CRYPTO.KEYRING VSE50 TLSV1.3 1
OTLS 192.168.22.150 990
*
SMNT LIBRARY PRD2
*
ATTACH SERVER-1
ATTACH SERVER-2
*
/*
```

Non-SSL Telnet Server

```
// EXEC BSTTVNET,SIZE=BSTTVNET
ID 01
*
OPEN 192.168.22.150 23
*
APPLID DBDCCICS CICS/TS AND ICCF
APPLID PRODCICS CICS/TS AND ICCF
APPLID V21VTAM2 OPTI-AUDIT VTAM Console Interface
APPLID BSTTUSST VTAM USS Table Emulation
APPLID BSTTVNET Printer Sharing Application
*
TITLE PTHVSE50 TELNET
*
TERMINAL T001 GENERIC
TERMINAL T002 GENERIC ** POOL GP1
TERMINAL T004 GENERIC ** POOL GP1
TERMINAL T005 SPECIFIC DBDCCICS
*
ATTACH TN3270E
/*
```

SSL Enabled Telnet Server

```
// EXEC BSTTVNET,SIZE=BSTTVNET
ID 01
*
XTLS CRYPTO.KEYRING VSE50 TLSV1.3 1 *
OTLS 192.168.22.150 992
*
APPLID DBDCCICS CICS/TS AND ICCF
APPLID PRODCICS CICS/TS AND ICCF
APPLID V21VTAM2 OPTI-AUDIT VTAM Console Interface
APPLID BSTTUSST VTAM USS Table Emulation
APPLID BSTTVNET Printer Sharing Application
*
TITLE PTHVSE50 TELNET OVER TLS
*
TERMINAL T001 GENERIC
TERMINAL T002 GENERIC ** POOL GP1
TERMINAL T004 GENERIC ** POOL GP1
TERMINAL T005 SPECIFIC DBDCCICS
*
ATTACH TN3270E
/*
```

```
// SETPARAM SSL$MIN='[TLSV1 | TLSV1.2 | TLSV1.3]'
```

```
// SETPARAM SSL$MAX='[TLSV1 | TLSv1.2 | TLSV1.3]'
```

```
// SETPARAM SSL$CPH='C027C014C013C012'
```

```
// SETPARAM SSL$DBG='[YES|NO]'
```

```
// SETPARAM BPX$GSK=IJBGSKOS & ENCRYPTION=STRONG in DFHSIT
```

```
// SETPARAM SSL$TRC='DD:lib.sublib(membername.membertype)'
```

```
// SETPARAM SSL$ICA='[YES|NO]'
```

```
// SETPARAM SSL$CSI='[YES|NO]'
```

```
// SETPARAM SSL$SSC='[FULL|QUIET|PARTIAL]
```

Q & A



Thank you!



Sources

- OpenSSL Library. (n.d.). OpenSSL Library. <https://openssl-library.org/>
- Wikipedia contributors. (2025, April 28). OpenSSL. Wikipedia. <https://en.wikipedia.org/wiki/OpenSSL>
- Wikipedia contributors. (2025a, April 26). Transport layer security. Wikipedia. https://en.wikipedia.org/wiki/Transport_Layer_Security
- Wikipedia-Autoren. (2003, July 29). Multiplexer. <https://de.wikipedia.org/wiki/Multiplexer>
- TCP/IP FOR VSE Optional Features Guide (2.3.3). (2024). CSI International. <https://app-na1.hubspotdocuments.com/documents/318822/view/752143089>
- IPv6/VSE SSL/TLS Installation, Programming and User's Guide. (2022). Barnard Software.