

Cleo[™] Cleossl V9.0
for CONVERSANT V8/R9
TN3270 SSL Host InterFace Extension
Quick Start Guide

This Quick Start Guide contains information about installing the Conversant V8/R9 version of the Cleo Cleossl V9.0 TN3270 SSL Host Interface Extension Package.

This Extension Package allows for connection via SSL to a TN3270 SSL Server

Important!

Read this document before installing and using the Cleo software. If you have questions about installing and using this product, contact Cleo Communications Technical Support between the hours of 8:30 A.M. and 5:00 P.M. (EST/EDT) at: 1.866.444.2536 or supportmi@cleo.com.

CL|E|O

Copyright © 2006 Cleo Communications

February 2006

Cleo Communications reserves the right to, without notice, modify or revise all or part of this document and/or change product features or specifications and shall not be responsible for any loss, cost or damage, including consequential damage, caused by reliance on these materials.

This document may not be reproduced, stored in a retrieval system or transmitted, in whole or in part, in any form or by any means (electronic, mechanical, photocopied or otherwise) without the prior written permission of Cleo Communications.

GOVERNMENT RESTRICTED RIGHTS

Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Use, reproduction or disclosure is subject to 52.227-19 (a) through (d) and restrictions set forth in the accompanying end user agreement.

GOVERNMENT LIMITED RIGHTS

Limited rights shall be effective indefinitely and are not subject to expiration as set forth in paragraph (3) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Copyright © 2006 Cleo Communications – All rights reserved.

Document No: 6512051

Version: 1.0

Trademark Acknowledgments

Cleo Communications has made every effort to accurately acknowledge all trademarks that appear in this document. Cleo Communications, however, cannot attest to the accuracy of this information.

Cleo™ is a trademark of Cleo Communications

CONVERSANT® System is a registered trademark of Avaya Inc.

UNIX® is a registered trademark licensed through X/Open Company Limited.

TABLE OF CONTENTS

Cleo Cleossl Installation.....	5
Cleo SSL SUPPORT INTRODUCTION.....	6
Installing Cleo Cleossl from CD.....	7
Installing Cleo Cleossl Without a CD.....	8
Basic Instructions for Configuring TN3270 SSL.....	9
Cleo Cleossl Removal.....	13
APPENDIX A.....	14

Cleo Cleossl Installation

Software Prerequisites:

- Unixware 7.1.1
- Avaya Conversant V8/R9
- IVR Designer or Script Builder.
- Cleo TN3270 V6.0.7.17, V6.0.7.16, V6.0.7.15, or V6.0.7.14
- Cleo vstndip V8.4, vstndip V8.5, Cleotndip V8.9 or Cleotdip V9.0.

Before the Cleossl Extended feature package can be installed, the following software must be installed and configured on the Avaya Conversant V8/R9 system having a connection to a 3270-mainframe host, using TN3270 protocol.

Cleo Host Dip Package vstndip – cleo vstndip V8.4 or V8.5 Package,

OR

Cleo Host Dip Package Ctnhdip – cleo Cleotndip V8.9 Package

OR

Cleo Host Dip Package Cleotdip - cleo Cleotdip V9.0

Cleo TN3270 Software Package cleotn – cleo TN3270(E) V6.0.7.1x

Note: Before installing Cleo Cleossl, please enter the following command:

```
# stop_vs    [wait for this step to complete; it will take several minutes]
```

Cleo SSL SUPPORT INTRODUCTION

Cleo's Cleossl software allows for a SSL connection to be made between the Cleo TN3270 Client emulator on the IVR and a TNSERVER that supports SSL connections. The tn3270 protocol data flows across the IVR and the TNSERVER connection, protected by SSL.

SSL is used to transport the tn3270 protocol data between the IVR and the TNSERVER. The Cleo tn3270 emulation software decrypts the SSL data as it arrives from the TNSERVER, and encrypts the data into SSL format as data is sent to the TNSERVER. As a result, the Host Applications on the IVR should not have to be changed when SSL is used.

After installing the “Cleossl” package, the user has various SSL configuration options, using the Cleo “tnconfig” utility.

1. The version of SSL to support, either 3.0 or 2.0.
In this mode no SSL certificates or keys are required. The Cleo tn3270 Client negotiates with the TNSERVER to determine the encryption methods to use.
2. Optionally, the full path to a Client Certificate File can be specified.
The certificate needs to be in PEM format(Privacy Enhanced Mail).
3. Optionally, the full path to a Client Key File can be specified.
The Key File needs to be in PEM format(Privacy Enhanced Mail).
4. Optionally, the full path to a file containing the Client Key File password can be specified.

So the Cleossl package does have, optional, support for a Client Certificate File, Key file, and Key file password.

Cleo uses the Openssl Projects toolkit. More information can be obtained at the Openssl Organization's Website

<http://www.openssl.org/>

More information about Version 3.0 of SSL can be obtained at the following Website

<http://wp.netscape.com/eng/ssl3/>

Installing Cleo Cleossl from CD

1. Login as *root*.
2. Enter the following commands:

```
# stop_vs  
  
# stop_hi
```
3. Create a mount-point for the CD if one does not already exist(/mnt is used as the mount-point in these instructions, but any empty directory can be used).
4. Insert the Cleo Cleossl V9.0 TN3270 SSL Host Interface Extension, for Avaya Conversant® V8/R9 CD into the CD ROM drive.
5. Mount the CD by entering the following command:

```
# /sbin/mount -F cdfs -r /dev/cdrom/cdrom1 /mnt
```
6. Start the Installation of the Cleossl Package

```
# pkgadd -d /mnt/Cleossl
```
7. Remove the CD from the drive. Store the CD in a safe place. It will be needed should you ever re-install the software.

Installing Cleo Cleossl Without a CD

1. Login as *root*.
2. If the "/voice1/cleo" directory does not already exist, create the directory to contain the Cleossl Host Interface Extension Software.

```
# cd /voice1  
  
# mkdir cleo  
  
# chmod 777 cleo
```

3. After unzipping the Cleossl Host Interface Extension binary Software file(CleosslV890cpio.zip), move the file to the Conversant V8 system and place it in the /voice1/cleo directory, and uncompress the file.

```
# cd /voice1/cleo  
  
# uncompress CleosslV890cpio.Z
```

4. Use the following command to move the Cleossl Host Interface Extension Software from the CleosslV890cpio file.

```
# cpio -ivBcdum < CleosslV890cpio
```

5. Start the Installation of the Cleossl Package

```
# pkgadd -d /voice1/cleo/Cleossl
```

Basic Instructions for Configuring TN3270 SSL

1. The TN3270 sessions start when the voice system starts. The program **tnconfig** must be executed to make the scripts for starting the TN3270 sessions. The **tnconfig** command has been enhanced to include various options to support SSL. See Appendix A. for specific options for the **tnconfig** command.

To use TN3270 sessions from a pool of lus on one host, and use SSL Version 3.0 with no Client SSL Certificates, execute **tnconfig** by entering the following command, and then **proceed to step 5**:

```
#tnconfig -h host name[:port id] -n number of lus -ssl 3
```

Note: The default portid is 23

A sample execution of tnconfig is as follows:

```
tnconfig -h tnsna -n 24 -ssl 3
```

Note: In this examples, the symbolic host name “**tnsna**” must be listed in the “**/etc/hosts**” file.

NOTE: Step 1 is the most common configuration method, for TN3270 with SSL Support.

2. **ONLY, if it is required,** to use TN3270 from pools of lus on multiple hosts, and use SSL Version 3.0 with no Client SSL Certificates, execute **tnconfig** by entering the following command, and then **proceed to step 5**:

```
#tnconfig -h host32701[:port id],host32702[:port id],host32703[:port id],host32704[:port id]-n #lus for host32701,#lus for host32702,#lus for host32703,#lus for host32704 -ssl 3
```

A sample execution of tnconfig is as follows:

```
tnconfig -h host32701,host32702,host32703,host32704 -n
24,10,10,24 -ssl 3
```

3. **ONLY, if it is required**, to use TN3270 sessions with specific LU Names on one host, and use SSL Version 3.0 with no Client SSL Certificates, execute **tnconfig** by entering the following command, and then **proceed to step 5**:

```
#tnconfig -h host name[:port id] -n number of lus -
l luname 1,luname 2,...,luname x -ssl 3
```

A sample execution of tnconfig is as follows:

```
tnconfig -h tnsna -n 32 -l lu1,lu2,...,lu32 -ssl 3
```

4. **ONLY, if it is required**, to use TN3270 sessions with specific LU Names on multiple hosts, and use SSL Version 3.0 with no Client SSL Certificates, execute **tnconfig** by entering the following command, and then **proceed to step 5**:

```
# tnconfig -h host name 1[:port id],host name 2[:port
id],...,host name x[:port id] -n number of lus for host
name 1,number of lus for host name 2,...,number of lus
for host name x -l luname 1 for host name 1,...,luname 1
for host name 2,...,luname 1 for host name x,...,luname
for last lu for host name x -ssl 3
```

A sample execution of tnconfig is as follows:

```
tnconfig -h host1,host2 -n 2,4 -l
lu1h1,lu2h1,lu1h2,lu2h2 -ssl 3
```

5. **If it is required to use SSL Version 2**, then use **-ssl 2**, in the examples above in place of **-ssl 3**., in addition to specifying.

A sample execution of tnconfig is as follows:

```
tnconfig -h tnsna -n 24 -ssl 2
```

6. **If it is required to use SSL compression** in addition to specifying SSL Version 2 or 3, the following option would be added to the **tnconfig** options, after the -ssl x argument.

-cm RLE|ZLIB

A sample execution of tnconfig is as follows:

```
tnconfig -h tnsna -n 24 -ssl 3 -cm ZLIB
```

7. **If it is required to use an SSL Client Certificate** in addition to specifying Version 2 or 3, the following option would be added to the **tnconfig** options, after the -ssl x argument.

-cc PATHTOCLIENTCERTIFICATEFILE

A sample execution of tnconfig is as follows:

```
tnconfig -h tnsna -n 24 -ssl 3 -cc /voicel/sslcert.pem
```

8. **If it is required to use a Key File** in addition to the Client Certificate, the following option would be added to the **tnconfig** options.

-ck PATHTOCLIENTKEYFILE

A sample execution of tnconfig is as follows:

```
tnconfig -h tnsna -n 24 -ssl 3 -cc /voicel/sslcert.pem  
-ck /voicel/sslkey.pem
```

9. If it is required to use a Password to the Key File and Client Certificate, the following option would be added to the **tnconfig** options.

-cp PATHTOCLIENTKEYFILEPASSWORDFILE

A sample execution of tnconfig is as follows:

```
tnconfig -h tnsna -n 24 -ssl 3 -cc /voicel/sslcert.pem
-ck /voicel/sslkey.pem -cp /voicel/sslpassword
```

10. **f there are specific TN3270 configuration requirements, not met in steps 1-4**, then configure the TN3270 software by changing the **com.txt** file to the specific requirements and converting the **config** file with the following commands (see the *TN3270 Administration Guide* for assistance on configuration):

```
# cd /opt/tn3270

# cp samples/tnsample.txt com.txt

# vi com.txt

# /opt/tn3270/bin/tncfgtcp com.txt
```

11. Perform an orderly shutdown(eg. **/etc/shutdown -y -g 0 -I 6**) to reboot the Solaris Sparc 8 operating system. Rebooting will start the voice system.
12. Assign IVR Designer application to each Host Session ID by entering the following command:

```
# hassign host_application to session_number[s]
```

Sample command:

```
# hassign vmtest to 0-32
```

13. Run the **hstatus** command to check status. The output will display the following:

<i>SESSION</i>	<i>SNA SERVER</i>	<i>Luname</i>	<i>SERVICE</i>	<i>STATE</i>
0	tn_server	-	Vmtest	LoggedIn
(voice Channel)	(name or IP address)	(N/A)	(ivr designer script)	(current state)

Cleo Cleossl Removal

1. Login as *root*
2. Remove the Cleossl Package by entering the following command:

```
# pkgrm Cleossl
```
3. Upon removal of the Cleossl package, the original configuration of the Cleo Host Interface, including TN3270, will be restored.

APPENDIX A.

TNCONFIG

The *tnconfig* command has the following options:

[-T TERMTYPE]

Optional parameter to specify a TN3270 Terminal Type to use. This sets the Environment Variable `OVERRIDE_TN3270_TERM` to the value of **TERMTYPE**.

[-NE]

Optional parameter to override the default of using TN3270 Extentions Mode.
If **-NE** is specified, then negotiations with TN SERVERS will not use TN3270 Extentions.

-h hostname1,hostname2,...,hostnamen

Mandatory parameter.

Each comma separated argument is an /etc/hosts entry or DNS name entry that points to a TNSERVER.

There must be a corresponding **-n** argument for each **-h** Argument.

-n number lus for hostname1,number lus for hostname2,...,number of lus for hostnamen

Mandatory parameter.

Each comma separated argument is the number of LUs to use for the corresponding **-h** argument.

**[-l 3270specificLUname1,3270specificLUname2,...,
3270specificLUnamen]**

Optional parameter.

Each comma separated argument is a specific LU name for TN3270. There will be an entry for every LU on every host/TNSERVER connection.

[-t seconds]

WHERE: *seconds* is the number of seconds to delay before trying to re-connect an LU, when a host connection fails.

The environment variable
SNA3270_RETRY_TIME
is set to the value of the *seconds* argument.

Optional parameter. 5 seconds is the default value.

The environment variable

SNA3270_RETRY_TIME

is set to the value of the *seconds* argument.

[-a seconds]

WHERE: *seconds* is the number of seconds to use for DIP HLLAPI no-response from emulator failure value

Optional parameter. 1 second is the default value.

[-ssl 3|2]

Optional parameter.

Where 3 specifies to use Version 3.0 of SSL to negotiate the SSL connection to the TNSERVER.

Where 2 specifies to use Version 2.0 of SSL to negotiate the SSL connection to the TNSERVER.

If the **-ssl** parameter is **NOT SPECIFIED**, then SSL will not be used to connect to the TNSERVER.

[-cm RLE|ZLIB]**Optional parameter.**

Where **RLE** specifies to use RLE type SSL compression.

Where **ZLIB** specifies to use ZLIB type SSL compression.

[-cc PATHTOCLIENTCERTIFICATEFILE]**Optional parameter.**

The specific path and file name of the Client SSL Certificate File must be specified. The File must be in "**Privacy Enhanced Mail**" format. This certificate file will be used when negotiating a SSL connection to the TNSERVER.

[-ck PATHTOCLIENTKEYFILE]**Optional parameter.**

The specific path and file name of the File that contains the KEY to the Client SSL Certificate.

The KEY File must be in "**Privacy Enhanced Mail**" format.

This KEY File will be used when the SSL Certificate is accessed, during the negotiation of a SSL connection to the TNSERVER.

[-cp PATHTOKEYFILEPASSWORDFILE]**Optional parameter.**

The specific path and file name of the File that contains the password needed to access the SSL KEY file.

The password in the KEY File Password File is used when the KEY File is accessed, during the negotiation of a SSL connection to the TNSERVER.