

The Cleo TN3270 SSL Software is available on Avaya Conversant V8.

The Cleo TN3270 SSL Software is a separate pkgadd package that has to be installed on top of existing Cleo Host Interface software:

- * For Avaya V8, Cleo Version 8.7 and above. Cleo is currently shipping Version 8.9 of its Host Interface Software, and Version 9.0 of the Cleossl Software.

During the TN3270 SSL Handshake negotiation between the Cleo Avaya IR TN3270 Client and the SSL TNSERVER/Mainframe, the encryption algorithm is determined.

The Cleo TN3270 Client supports the following encryption algorithms

- DES-CBC
- DES-EDE3-CBC
- IDEA-CBC
- RC4
- RC2-CBC
- AES-128-CBC
- AES-192-CBC
- AES-256-CBC
- MD2
- RSA-MD2
- MD5
- RSA-MD5
- SSL2-MD5
- SSL3-MD5
- SHA1
- RSA-SHA1
- SSL3-SHA1
- RSA-SHA1-2
- DSA
- DSA-SHA1
- DSA-SHA1-OLD
- DSS1

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.
We have actually connected to a Major Bank's SSL TNSERVER using Version 3.0 SSL, successfully.
No other certificates or keys were used.

The Cleo SSL TN3270 software negotiated with the Bank's SSL TNSERVER to decide on encryption options, etc.
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/>

The commands that have been added to the Cleo "tnconfig" utility are shown below:

FOR TN3270 WITH SSL ENABLED

```
tnconfig [-T TERMTYPE] [-NE] -h host[:portid] -n nlu -ssl 3|2
          [-cm RLE|ZLIB] (compression method)
          [-cc PATHTOCLIENTCERTIFICATEFILE]
          [-ck PATHTOCLIENTKEYFILE]
          [-cp PATHTOCLIENTKEYFILEPASSWORDFILE]
          [-l luname,...]
```

Example: tnconfig -h tnsna -n 24 -ssl 3

Example: tnconfig -h tnsna -n 24 -ssl 3 -cm RLE -cc /export/sslcert.pem
-ck /export/sslclient.pem -cp /export/sslpassword