

DCMTK - Feature #713

TCP/IP and TLS Connection Parameters are not dumped for most networking tools

2017-01-25 12:51 - Jörg Riesmeier

Status:	New	Start date:	2017-01-25
Priority:	Normal	Due date:	
Assignee:		% Done:	10%
Category:	Library and Apps	Estimated time:	0:00 hour
Target version:		Compiler:	
Module:	dcmnet and others?		
Operating System:			

Description

There is a DcmTransportConnection::dumpConnectionParameter() method and also a DUL_DumpConnectionParameters() and a ASC_dumpConnectionParameters() function, but none of these seem to be used for most of the networking tools.

One of the few exceptions are storescu, dcmpssnd and dcmpsrcv, which all use ASC_dumpConnectionParameters().

Dumping the connection parameters is especially useful in the context of a secure TLS connection. Here's an example output of storescu:

```
[...]
D: Parsing an A-ASSOCIATE PDU
D: Transport connection: TLS/SSL over TCP/IP
D:   Protocol: TLSv1
D:   Ciphersuite: AES128-SHA, version: TLSv1/SSLv3, encryption: 128 bits
D: X.509v3 Certificate
D:   Subject      : /C=DE/ST=Lower Saxony/L=Oldenburg/O=J. Riesmeier/OU=DCMTK/CN=My Cert/emailAddress=mycert/at/jriesmeier.com
D:   Issued by    : /C=DE/ST=Lower Saxony/L=Oldenburg/O=J. Riesmeier/OU=DCMTK/CN=My CA/emailAddress=myca/at/jriesmeier.com
D:   Serial no.   : 1
D:   Validity     : not before Jan 25 10:58:30 2017 GMT, not after Jan 25 10:58:30 2019 GMT
D:   Public key   : RSA, 2048 bits
D:
D:
D: Association Parameters Negotiated:
[...]
```

~~The extra newlines at the end of the TLS part of the output should also be removed.=> done~~

History

#1 - 2017-01-25 13:29 - Jörg Riesmeier

- Description updated

#2 - 2017-01-26 12:16 - Jörg Riesmeier

- Target version deleted (3.6.2)

- % Done changed from 0 to 10