DCMTK - Bug #799

DCMTK 3.6.2 TLS binaries for Windows do not support 3DES

2017-11-03 09:41 - Marco Eichelberg

Status:	Closed	**Start date:**	2017-11-03
Priority:	High	**Due date:**	
Assignee:	Jan Schlamelcher	**% Done:**	100%
Category:	Application	**Estimated time:**	0:00 hour
Target version:	3.6.3		
Module:		**Compiler:**	
Operating System:	Windows		

Description

The TLS-enabled Windows binaries for DCMTK 3.6.2 have been compiled with OpenSSL 1.1.0.
OpenSSL 1.1.0 by default does not support 3DES ciphers anymore, these have to be explicitly enabled at compile time by configuring OpenSSL with the “enable-weak-ssl-ciphers” option.
However, the DICOM Basic Security Profile still uses 3DES (TLS_RSA_WITH_3DES_EDE_CBC_SHA), therefore updated binaries with enabled 3DES support should be provided
(and the internal OpenSSL nightly build should be adapted accordingly).

See also: https://www.openssl.org/blog/blog/2016/08/24/sweet32/

History

#1 - 2018-02-09 11:38 - Jan Schlamelcher

- Status changed from New to Closed

- % Done changed from 0 to 100

The OpenSSL binaries for release 3.6.3 were built with the “enable-weak-ssl-ciphers” option and the Windows DCMTK binaries have be built using these OpenSSL binaries. Tests showed that DCMTK binaies don't need to be recompiled for enabling TLS_RSA_WITH_3DES_EDE_CBC_SHA anyway, replacing the OpenSSL DLLs is sufficient.