DCMTK - Bug #865

Fix TLS 1.3 ciphersuite selection when using OpenSSL 1.1.1

2019-01-02 17:14 - Marco Eichelberg

Status:	Closed	**Start date:**	2019-01-02
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library	**Estimated time:**	0:00 hour
Target version:	3.6.5		
Module:	dcmtls	**Compiler:**	
Operating System:			

Description

OpenSSL 1.1.1 has introduced new APIs for managing TLS 1.3 ciphersuites, which are handled completely separate from the older SSL3 and TLS 1.0-1.2 ciphersuites.

This leads to unexpected behaviour in DCMTK: A connection between echoscu --profile-null and storescp --profile-bcp195-nd should normally fail, because storescp should refuse to negotiate the NULL cipher. When using OpenSSL 1.1.1, however, the connection succeeds because a TLS 1.3 cipher is selected instead. While the connection is arguably secure, this is not what a user would expect when explicitly asking for the NULL (unencrypted) ciphersuite, and it breaks several of DCMTK's integration test cases.

The dcmtls module should be modified such that when compiling with OpenSSL 1.1.1 or newer,

- TLS 1.3 support is disabled for the historic DICOM security profiles (3DES, AES, NULL)
- TLS 1.3 support is enabled for the newer DICOM security profiles, but ciphersuites are restricted to those that fulfill the BCP195 requirements.

History

#1 - 2019-03-04 18:31 - Marco Eichelberg

- Status changed from New to Closed

- Assignee set to Marco Eichelberg

- % Done changed from 0 to 100

Closed by commit #b9e37ae60.