DCMTK - Conformance #1030

DICOM supplement 230 replaces all TLS profiles

2022-07-20 08:40 - Marco Eichelberg

Status:	Closed	**Start date:**	2022-07-20
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library and Apps	**Estimated time:**	25:00 hours
Target version:	3.6.8		
Module:	dcmtls	**Compiler:**	
Operating System:			

Description

With DICOM supplement 230 (in public comment as of July 2022), all existing TLS profiles will be retired and replaced by two new TLS profiles:

- BCP 195 RFC 8996 TLS Secure Transport Connection Profile
- Extended BCP 195 RFC 8996 TLS Secure Transport Connection Profile

This will require implementation of the new profiles in the dcmtls module and appropriate command line options in all command line tools that support TLS.

The difference between the current "Non-Downgrading BCP 195 TLS Secure Transport Connection Profile" and the new "BCP 195 RFC 8996 TLS Secure Transport Connection Profile" seem to be very small. It seems that the only differences are that TLS 1.3 **must** now be preferred over TLS 1.2 when both are available (which we do anyway), and that additional ciphersuites may only be supported if they are of similar or greater strength than the four default ones. (Note that this analysis is based on the public comment version, not the final text)

The differences between the two Extended profiles have to be analyzed in more detail.

History

#1 - 2023-01-16 16:11 - Jörg Riesmeier

- Assignee set to Marco Eichelberg

- Target version set to 3.6.8

#2 - 2023-03-06 18:27 - Marco Eichelberg

- Category set to Library and Apps

- Status changed from New to Closed

- % Done changed from 0 to 100

- Estimated time set to 25:00 h

Closed by commit #d269161f7 (public DCMTK) and #89d522e0c (private modules).