DCMTK - Feature #973

Allow TLS 1.0 and 1.1 to be disabled in BCP 195 profile

2021-03-12 10:41 - Marco Eichelberg

Status:	Closed	**Start date:**	2021-03-12
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:		**Estimated time:**	1:00 hour
Target version:			
Module:	dcmtls	**Compiler:**	
Operating System:			

Description

The default security profile in DCMTK is the "BCP 195 profile" (--profile-bcp195). Currently DCMTK by default negotiates TLS 1.0 or newer for this profile, in order to offer backward compatibility to the older AES profile. A recent publication by the NSA recommends that TLS 1.0 and 1.1 should be disabled because they are sufficiently broken to be considered insecure (see attachment). The non-downgrading and extended BCP 195 profiles already do that, but for the default BCP 195 profile this should be made configurable (e.g. an option like "--enable-backward-compatibility" would enable support for the historic AES ciphersuite and TLS 1.0/1.1, which should be off by default and only enabled when needed for compatibility reasons).

History

#1 - 2021-04-24 15:06 - Marco Eichelberg

- Assignee set to Marco Eichelberg

A second look at the existing code in dcmtls shows that we already have all options that we need:

- the non-downgrading BCP 195 profile disables TLS 1.0, TLS 1.1 and the AES ciphersuite that provides backward compatibility to the historic AES profile
- the BPC 195 profile enables a fallback to TLS 1.0 and TLS 1.1 and provides backward compatibility to the historic AES profile

In terms of the IHE IT-I Technical Framework, the non-downgrading BCP 195 profile implements the "TLS 1.2 floor using BCP195 Option", and the BCP 195 profile implements the "TLS 1.0 Floor using BCP195 Option". One could think of a BCP 195 profile that supports TLS 1.0 and TLS 1.1 but does not support AES, but since TLS 1.0 and 1.1 must both be considered broken, this is not a desirable implementation choice anyway.

Therefore, the best approach is simply to change the default TLS profile from BCP 195 to the non-downgrading BCP 195 profile.

#2 - 2021-04-24 15:33 - Marco Eichelberg

- Status changed from New to Closed

- % Done changed from 0 to 100

- Estimated time set to 1:00 h

Closed by commit #ce7518d12 (public DCMTK) and #4dccefdf4 (private modules).

Files

ELIMINATING_OBSOLETE_TLS_UOO197443-20.PDF	288 KB	2021-03-12	Marco Eichelberg