DCMTK - Conformance #792

Implement support for the new TLS Security Profiles (Supplement 204)

2017-09-26 09:08 - Marco Eichelberg

Status:	Closed	**Start date:**	2017-09-26
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Library and Apps	**Estimated time:**	0:00 hour
Target version:			
Module:	dcmtls	**Compiler:**	
Operating System:			

Description

Two new Secure Connection profiles are added to make DICOM consistent with the latest RFCs and best practices for TLS security. These are:

1. A Best Practices TLS Profile that requires compliance with the IETF BCP 195 Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). This profile requires that TLS negotiation start with the strong security protection parameters, and allows progressive negotiation of weaker protection down to a minimum protection limit.
2. A Non-Downgrading Best Practices TLS Profile that does not permit negotiation of weaker protections. This profile will refuse a connection that is not the initial strong level of protection.
   The old Basic TLS Secure Transport Connection Profile is retired. IETF considers it inadequate security, because the methods for breaking in are well known. Implementations that use it will not interoperate with the Best Practices TLS Profile.

The old AES TLS Secure Transport Connection Profile is retired. Implementations that use it will not interoperate with the Non-Downgrading Best Practices TLS Profile. Implementations that use it will interoperate with the Best Practices TLS Profile because it is acceptable as one of the lower levels of protection that can be negotiated.

Related issues:

Related to DCMTK - Feature #812: Update list of supported TLS ciphersuites in...	**Closed**	**2018-02-13**

History

#1 - 2018-04-25 10:00 - Jörg Riesmeier

- Related to Feature #812: Update list of supported TLS ciphersuites in DCMTK added

#2 - 2018-05-02 11:32 - Marco Eichelberg

- Status changed from New to Closed

- % Done changed from 0 to 100

Closed by commits #bd4f159 to #e54a53a.