DCMTK - Feature #959

Enable dcmtls to only accept a fixed list of client certificates

2021-01-12 16:48 - Marco Eichelberg

Status:	New	**Start date:**	2021-01-12
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Library and Apps	**Estimated time:**	0:00 hour
Target version:			
Module:	dcmtls	**Compiler:**	
Operating System:			

Description

Currently, the TLS implementation in dcmtls always accepts all certificates issued by a CA that is configured as trustworthy.
In practical settings, it might be useful to further restrict this. For example, a modality only needs to communicate with the RIS and the PACS, but never with any other TLS-enabled system.
It would be nice if an explicit list of client certificates could be defined as the only ones that are to be trusted. This can be implemented in
DcmTLSTransportLayer_certificateValidationCallback() in dcmtls/libsrc/tlslayer.cc, which is a callback function that OpenSSL calls after each
certification verification operation. This function can do additional checks and revise the result of the certificate verification.
The function could, for example, look up the client certificate in a hashed directory of "acceptable" client certificates and return "false" if the certificate is not found there.

Note: One implementation strategy to be considered is whether in this case the result of the callback should completely replace OpenSSL's test results (which would mean that client certificates could be placed in the "acceptable" list even if their root CA certificate is not available, but might also cause expired certificates to be accepted) or only amend it (by setting the test result from true to false if the certificate is not found in the explicit list, but not vice versa).

Related issues:

Has duplicate DCMTK - Feature #979: Add support for the IHE "Direct certifica...	**New**	**2021-04-04**

History

#1 - 2023-01-16 16:21 - Jörg Riesmeier

- Has duplicate Feature #979: Add support for the IHE "Direct certificate validation" mode of certificate validation in the dcmtls module added