DCMTK - Feature #979

Add support for the IHE "Direct certificate validation" mode of certificate validation in the dcmtls module

2021-04-04 13:18 - Marco Eichelberg

Status:	New	**Start date:**	2021-04-04
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Library and Apps	**Estimated time:**	0:00 hour
Target version:			
Module:	dcmtls	**Compiler:**	
Operating System:			

Description

The IHE IT-Integration Technical Framework specifies two alternative certificate validatation strategies for Secure Node/Secure Applications. The first one, "certificate validation based on signature by a trusted CA", is supported by DCMTK's dcmtls module, while the second one, "direct certificate validation to a set of trusted certificates" is not.

3.19.6.1.2 Direct certificate validation
The Secure Node or Secure Application:

- Shall provide means for installing of the required certificates, for example, via removable media or network interchange (where the set of trusted certificates can be a mixture of CA signed certificates and self-signed certificates).
- Shall support digital certificates encoded using both Deterministic Encoding Rules (DER) and Basic Encoding Rules (BER).
- Shall accept communications for which there is a certificate configured as acceptable for direct certificate validation.

This should be implemented as an option in dcmtls.

Note that there is already a dummy function DcmTLSTransportLayer_certificateValidationCallback() in tlslayer.cc which could be used to implement this kind of certificate validation, e.g. against a directory of explicitly permitted certificate files. It should be configurable whether these certificates are accepted even if they cannot be validated against a CA root, or whether both a successful validation of the CA chain AND the presence of the certificate in that directory are required for the certificate to pass the test. This could be another option.

Related issues:

Is duplicate of DCMTK - Feature #959: Enable dcmtls to only accept a fixed li...	**New**	**2021-01-12**

History

#1 - 2021-04-04 13:20 - Marco Eichelberg

- Tracker changed from Bug to Feature

#2 - 2023-01-16 16:21 - Jörg Riesmeier

- Is duplicate of Feature #959: Enable dcmtls to only accept a fixed list of client certificates added