DCMTK - Feature #978

Add support for the IHE "FQDN Validation of Server Certificate Option" in the dcmtls module

2021-04-04 13:08 - 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 the following option for Secure Node/Secure Application, which is currently not supported by DCMTK:

3.19.6.1.4 FQDN Validation of Server Certificate Option
A client, who is validating a server's identity, shall validate that the reference identifier present in a subjectAltName entry of type DNS-ID matches the source domain of the server, per 3735 RFC6125 Section 6. Note that the rules described in RFC6125 Section 6 require the validation to be performed based on the input source and the DNS-ID fully-qualified domain name. In an environment where clients have implemented this option, a server's X.509 certificate shall contain a subjectAltName entry of type DNS-ID, per RFC6125 Section 4.

This should be implemented as an option in dcmtls.

History

#1 - 2021-04-04 13:09 - Marco Eichelberg

- Category set to Library and Apps

- Module set to dcmtls