DCMTK - Feature #922

Implement OCSP in dcmsign

2020-01-01 18:51 - Marco Eichelberg

Status:	New	**Start date:**	2020-01-01
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Library and Apps	**Estimated time:**	0:00 hour
Target version:			
Module:	dcmsign	**Compiler:**	
Operating System:			

Description

Starting with DCMTK 3.6.6, the dcmsign module can check a certificate revocation list (CRL) when verifying the signer certificate of a signature.

A common alternative to CRLs is the Online Certificate Status Protocol (OCSP) specified in RFC 6960, where the validity of a certificate is checked online by accessing the OCSP service (HTTP/HTTPS based) provided by the CA. For CAs supporting this service, the URL of the OCSP server is encoded in each certificate, using the *Authority Information Access* extension.

This should also be supported in dcmsign, since OpenSSL provides an implementation of the protocol.