DCMTK - Feature #921

Improve handling of Certificate Revocation Lists (CRLs) in dcmsign

2020-01-01 18:40 - 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) for each CA certificate when dcmsign is run with --add-crl-file or --enable-crl-vfy. Currently, the verification of a signature will fail if the signer certificate is on the revocation list.

The code should be extended to consider the date and time at which a certificate was revoked (this information is provided for each revoked certificate in the CRL). Signatures created *before* the revocation should be considered valid. Since the DICOM DigitalSignatureDateTime attribute value is easy to forge, this rule should only apply if a certified timestamp is present, and the timestamp was created before the signer certificate was revoked. The appropriate place for the implementation is in SiCertificateVerifier::verifyCallback() (dcmsign/libsrc/sicertvf.cc).

Furthermore, CRLs provide a "Next Update" attribute that contains the date and time when a new version of the CRL will be made available by the CA. CRLs may also contain a URL where the latest version of the CRL can be downloaded (in the *Authority Information Access* extension). This information is currently ignored by dcmsign. At least a warning should be printed when the CRL is outdated, together with the download URL (if present).