DCMTK - Feature #920

Implement Socket based RFC 3161 Time-Stamp Protocol in dcmsign

2020-01-01 18:12 - 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 create timestamp requests, read timestamp responses and insert the timestamp into attribute (0400,0310) CertifiedTimestamp of the DigitalSignaturesSequence, and verify certified timestamps when verifying a digital signature. However, currently only the file-based protocol defined in RFC 3161 section 3.2 is implemented.

Support for the Socket based online timestamp protocol defined in RFC 3161 section 3.3 should also be implemented. The implementation should support both plain (unprotected) and TLS protected connections, since some timestamp providers (e.g. http://www.globaltrust.eu/) implement the Socket based protocol over TLS.

History

#1 - 2020-01-01 18:12 - Marco Eichelberg

- Subject changed from Implement HTTP-based RFC 3161 Time-Stamp Protocol in dcmsign to Implement Socket based RFC 3161 Time-Stamp Protocol in dcmsign