DCMTK - Feature #919

Implement HTTP-based RFC 3161 Time-Stamp Protocol in dcmsign

2020-01-01 18:07 - 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 HTTP/HTTPS-based online timestamp protocol defined in RFC 3161 section 3.4 should also be implemented.

Note that this protocol can be simulated using the "curl" tool:

```
dcmsign --sign key.pem cert.pem --timestamp-file example.tsq example.uid input.dcm temp.dcm
curl -H "Content-Type: application/timestamp-query" --data-binary '@example.tsq' https://freetsa.org/tsr > example.tsr
dcmsign --insert-timestamp example.tsq example.tsr example.uid temp.dcm signed.dcm
```