DCMTK - Feature #1064

Add support for TLS Servername Indication (SNI) in DCMTK

2023-02-06 11:55 - Marco Eichelberg

Status:	Closed		**Start date:**	2023-02-06
Priority:	Normal		**Due date:**	
Assignee:	Marco Eichelberg		**% Done:**	100%
Category:	Library and Apps		**Estimated time:**	0:00 hour
Target version:	3.6.9			
Module:	dcmtls		**Compiler:**	
Operating System:				

Description

With TLS Server Name Indication (SNI), a TLS server can have multiple certificates installed on the same IP address. SNI-capable clients will specify the hostname of the server they're trying to reach during the initial handshake process. This allows the TLS server to determine the correct certificate to use for the connection.

It would be a useful extension to DCMTK's TLS clients to add a command line enabling SNI. In OpenSSL, this might be as simple as calling the following function:
int SSL_set_tlsext_host_name(const SSL *s, const char *name);

Suggested 2023-02-03 by Yi Lu <digihunch@gmail.com>.

History

#1 - 2024-06-26 10:46 - Jörg Riesmeier

- Status changed from New to Closed

- Assignee set to Marco Eichelberg

- Target version set to 3.6.9

- % Done changed from 0 to 100

Closed with commit fcfa55a5d.