

DCMTK - Feature #1080

Introduce new --list-profiles option to TLS-enabled network tools

2023-06-22 14:56 - Jörg Riesmeier

Status:	Closed	Start date:	2023-06-22
Priority:	Normal	Due date:	
Assignee:	Marco Eichelberg	% Done:	100%
Category:	Library and Apps	Estimated time:	2:00 hours
Target version:	3.7.1+	Compiler:	
Module:	dcmTLS, dcmnet		
Operating System:			
Description <p>A new command line option --list-profiles could be introduced that lists all implemented Secure Transport Connection Profiles and indicates for each of them whether they are actually supported (e.g. by the underlying OpenSSL library) or not. This way, it would be easier than now to check to which security profiles a tool is compliant.</p> <p>That means, something like the following:</p> <pre>Cryptographic algorithms implemented by: OpenSSL 3.0.2</pre> <p>Supported Secure Transport Connection Profiles:</p> <pre>BCP 195 TLS Secure Transport Connection Profile- (retired) Non-Downgrading BCP 195 TLS Secure Transport Connection Profile- (retired) Extended BCP 195 TLS Profile Secure Transport Connection Profile- (retired) BCP 195 RFC 8996 TLS Secure Transport Connection Profile-</pre> <p>Not supported Secure Transport Connection Profiles:</p> <pre>Basic TLS Secure Transport Connection Profile- (retired) = not supported by OpenSSL 3.0.2 ISCL Secure Transport Connection Profile- (retired) = not implemented Modified BCP 195 RFC 8996 TLS Secure Transport Connection Profile- = not supported by OpenSSL 3.0.2</pre>			

History

#1 - 2024-11-25 11:26 - Marco Eichelberg

- Status changed from New to Closed
- Assignee set to Marco Eichelberg
- % Done changed from 0 to 100
- Estimated time set to 2:00 h

Closed by commits #1ac38b285 (public DCMTK) and #29f7a9ffb (private modules).