DCMTK - Feature #636

Add warning/hint to dcmtls about non-standard ciphersuites

2015-04-17 11:01 - Michael Onken

Status:	Closed	**Start date:**	2015-04-17
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Documentation	**Estimated time:**	0:00 hour
Target version:			
Module:	dcmtls, dcmnet	**Compiler:**	
Operating System:			

Description

Add warning/hint to dcmtls about non-standard ciphersuites in order to bring attention to the user which ciphersuites are not available in DICOM at all (but selectable through dcmtls/openssl) and using those ciphersuites this may lead to insecure applications.

History

#1 - 2015-04-17 13:03 - Jörg Riesmeier

- Category set to Documentation

- Module set to dcmtls, dcmnet

#2 - 2018-05-02 11:38 - Marco Eichelberg

- Status changed from New to Closed

- % Done changed from 0 to 100

This has been addressed in the revision of the dcmtls module: The manual selection of ciphersuites that do not comply with the recommendations of BCP 195 (RFC 7525) cause a warning to be printed.
Closed by commit #bd4f159.