DCMTK - Bug #863

dcmtls error related to elliptic curves on RHEL 7.6

2018-12-13 15:53 - Marco Eichelberg

Status:	Closed	**Start date:**	2018-12-13
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library and Apps	**Estimated time:**	0:00 hour
Target version:	3.6.5		
Module:	dcmtls	**Compiler:**	
Operating System:			

Description

When starting DCMTK 3.6.4 dcmtls based applications on RHEL 7.6 (OpenSSL 1.0.2), the following error message is printed:

```
ERROR: unable to configure the TLS Supported Elliptic Curves extension.
```

Apparently the OpenSSL library in RHEL does not support the 17 elliptic curves supported in a standard OpenSSL 1.0.2 installation. „openssl ecparam -list_curves“ only reports the following curves

```
  secp256k1 : SECG curve over a 256 bit prime field
  secp384r1 : NIST/SECG curve over a 384 bit prime field
  secp521r1 : NIST/SECG curve over a 521 bit prime field
  prime256v1: X9.62/SECG curve over a 256 bit prime field
```

dcmtls should probably check at runtime which elliptic are really supported by the OpenSSL library and only activate these.

History

#1 - 2018-12-13 15:54 - Marco Eichelberg

Bug reported by Peter Klotz <Peter.Klotz@ith-icoserve.com>

#2 - 2019-01-24 13:07 - Marco Eichelberg

- Status changed from New to Closed

- % Done changed from 0 to 100

Closed by commit #caf1f88b4.