ScalES-PPM - Feature #344

Add support for OpenSSL 1.1.0 crypto

09/25/2017 07:24 PM - Matthew Krupcale

Status:	Closed	**Start date:**	09/25/2017
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:		**Estimated time:**	0:00 hour
Target version:			

Description

src/crypto/ppm_checksum_c.c was designed around the pre-1.1.0 OpenSSL API and uses a stack-allocated digest context, EVP_MD_CTX. In the post-1.1.0 OpenSSL API (in particular, after commit 7638370ca6cb1d89eba5d891f522776b9da3d6e7), the EVP_MD_CTX type was made opaque and must be dynamically allocated using the new EVP_MD_CTX_{new,free} functions (renamed from EVP_MD_CTX_{create,destroy} in commit 959ed5316c84d0e12ad18acfd40cefe15603ddfb).

The attached patch uses the old method for OPENSSL_VERSION_NUMBER < 0x1010000fL and uses the new methods otherwise. It also uses the recommended EVP_Digest{Init,Final}_ex functions rather than the EVP_Digest{Init,Final} counterparts which perform additional initialization and cleanup on mdctx and are unnecessary since we are explicitly initializing and freeing the digest contexts within the scope of the PPM_checksum function--see OpenSSL doc/man3/EVP_DigestInit.pod for details. Finally, the patch also does explicit checking for the success or failure of the EVP_Digest functions and aborts if there is a failure.

History

#1 - 08/05/2020 09:26 AM - Thomas Jahns

- Status changed from New to Resolved

- % Done changed from 0 to 100

This issue was addressed in commit:17317332d1485a4, part of release 1.0.6.

#2 - 03/18/2022 10:07 AM - Thomas Jahns

- Status changed from Resolved to Closed

Files

scales-ppm-ppm_checksum_c.c-openssl-1.1.0.patch	2.04 KB	09/25/2017	Matthew Krupcale