

## Lasso - Development #74996

### Use EVP\_\* in a way that is compatible with OpenSSL 1.0

01 mars 2023 18:05 - Maxime Besson

<b>Statut:</b>	Fermé	<b>Début:</b>	01 mars 2023
<b>Priorité:</b>	Normal	<b>Echéance:</b>	
<b>Assigné à:</b>	Maxime Besson	<b>% réalisé:</b>	0%
<b>Catégorie:</b>		<b>Temps estimé:</b>	0:00 heure
<b>Version cible:</b>		<b>Planning:</b>	Non
<b>Patch proposé:</b>	Non		

#### Description

Hi,

I am trying to build Lasso on CentOS 7:

```
OpenSSL 1.0.2k-fips 26 Jan 2017
```

Unfortunately, with this version:

- EVP\_DigestSign does not exist
- EVP\_MD\_CTX\_free does not exist

which leads to compilation/linking errors. As mentioned on the mailing list, building against EPEL-provided OpenSSL 1.1 leads to segfaults (and is not a great approach anyway, as it makes Lasso depend on EPEL).

Both issues are pretty easy to fix: EVP\_DigestSign should be equivalent to EVP\_DigestSignUpdate + EVP\_DigestSignFinal, and EVP\_MD\_CTX\_free is an alias for EVP\_MD\_CTX\_destroy

I have attached a patch that I tested successfully (using the LemonLDAP::NG unit test suite) on both OpenSSL 1.0 and OpenSSL 3.0

#### Révisions associées

##### Révision 7ac76525 - 06 mars 2023 11:44 - Benjamin Dauvergne

Compatibility with EVP API of openssl 1.x (#74996)

Thanks to Maxime Besson from Worteks.

##### Révision d4578864 - 14 mars 2023 18:14 - Benjamin Dauvergne

Release 2.8.2 (#74996)

- Compatibility with EVP API of openssl 1.x, thanks to Maxime Besson from Worteks.

#### Historique

##### #1 - 01 mars 2023 19:06 - Benjamin Dauvergne

- Statut changé de Nouveau à En cours

- Assigné à mis à Benjamin Dauvergne

Looks good, I will make a 2.8.2 release soon.

##### #2 - 17 mars 2023 08:25 - Benjamin Dauvergne

- Statut changé de En cours à Fermé

- Assigné à changé de Benjamin Dauvergne à Maxime Besson

Lasso 2.8.2 released.

#### Fichiers

openssl-1\_0.diff

3,07 ko

01 mars 2023

Maxime Besson