



*Full credit is given to the above companies including the OS that this PDF file was generated!*

***Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP\_KDF-PKCS12KDF.7ossl'***

***\$ man EVP\_KDF-PKCS12KDF.7ossl***

EVP\_KDF-PKCS12KDF(7ossl)      OpenSSL      EVP\_KDF-PKCS12KDF(7ossl)

**NAME**

EVP\_KDF-PKCS12KDF - The PKCS#12 EVP\_KDF implementation

**DESCRIPTION**

Support for computing the PKCS#12 password-based KDF through the EVP\_KDF API.

The EVP\_KDF-PKCS12KDF algorithm implements the PKCS#12 password-based key derivation function, as described in appendix B of RFC 7292 (PKCS #12: Personal Information Exchange Syntax); it derives a key from a password using a salt, iteration count and the intended usage.

**Identity**

"PKCS12KDF" is the name for this implementation; it can be used with the EVP\_KDF\_fetch() function.

## Supported parameters

The supported parameters are:

"pass" (OSSL\_KDF\_PARAM\_PASSWORD) <octet string>

"salt" (OSSL\_KDF\_PARAM\_SALT) <octet string>

"iter" (OSSL\_KDF\_PARAM\_ITER) <unsigned integer>

"properties" (OSSL\_KDF\_PARAM\_PROPERTIES) <UTF8 string>

"digest" (OSSL\_KDF\_PARAM\_DIGEST) <UTF8 string>

These parameters work as described in "PARAMETERS" in EVP\_KDF(3).

"id" (OSSL\_KDF\_PARAM\_PKCS12\_ID) <integer>

This parameter is used to specify the intended usage of the output

bits, as per RFC 7292 section B.3.

## NOTES

A typical application of this algorithm is to derive keying material for an encryption algorithm from a password in the "pass", a salt in "salt", and an iteration count.

Increasing the "iter" parameter slows down the algorithm which makes it harder for an attacker to perform a brute force attack using a large number of candidate passwords.

No assumption is made regarding the given password; it is simply treated as a byte sequence.

## CONFORMING TO

RFC7292

## SEE ALSO

EVP\_KDF(3), EVP\_KDF\_CTX\_new(3), EVP\_KDF\_CTX\_free(3),  
EVP\_KDF\_CTX\_set\_params(3), EVP\_KDF\_derive(3), "PARAMETERS" in  
EVP\_KDF(3)

## HISTORY

This functionality was added to OpenSSL 3.0.

## COPYRIGHT

Copyright 2020 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.

3.0.7                    2023-07-13            EVP\_KDF-PKCS12KDF(7ossl)