



Full credit is given to the above companies including the Operating System (OS) that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP_KDF-PKCS12KDF.7ssl'

\$ man EVP_KDF-PKCS12KDF.7ssl

EVP_KDF-PKCS12KDF(7SSL) OpenSSL EVP_KDF-PKCS12KDF(7SSL)

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>>.

3.0.2

2024-02-16

EVP_KDF-PKCS12KDF(7SSL)