



*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\_OpenUpdate.3ossl'***

***\$ man EVP\_OpenUpdate.3ossl***

EVP\_OPENINIT(3ossl)            OpenSSL            EVP\_OPENINIT(3ossl)

#### NAME

EVP\_OpenInit, EVP\_OpenUpdate, EVP\_OpenFinal - EVP envelope decryption

#### SYNOPSIS

```
#include <openssl/evp.h>

int EVP_OpenInit(EVP_CIPHER_CTX *ctx, EVP_CIPHER *type, unsigned char *ek,
                int ekl, unsigned char *iv, EVP_PKEY *priv);

int EVP_OpenUpdate(EVP_CIPHER_CTX *ctx, unsigned char *out,
                  int *outl, unsigned char *in, int inl);

int EVP_OpenFinal(EVP_CIPHER_CTX *ctx, unsigned char *out, int *outl);
```

#### DESCRIPTION

The EVP envelope routines are a high-level interface to envelope decryption. They decrypt a public key encrypted symmetric key and then decrypt data using it.

EVP\_OpenInit() initializes a cipher context ctx for decryption with cipher type. It decrypts the encrypted symmetric key of length ekl bytes passed in the ek parameter using the private key priv. The IV is supplied in the iv parameter.

EVP\_OpenUpdate() and EVP\_OpenFinal() have exactly the same properties as the EVP\_DecryptUpdate() and EVP\_DecryptFinal() routines, as documented on the EVP\_EncryptInit(3) manual page.

## NOTES

It is possible to call EVP\_OpenInit() twice in the same way as EVP\_DecryptInit(). The first call should have priv set to NULL and (after setting any cipher parameters) it should be called again with type set to NULL.

If the cipher passed in the type parameter is a variable length cipher then the key length will be set to the value of the recovered key length. If the cipher is a fixed length cipher then the recovered key length must match the fixed cipher length.

## RETURN VALUES

EVP\_OpenInit() returns 0 on error or a non zero integer (actually the recovered secret key size) if successful.

EVP\_OpenUpdate() returns 1 for success or 0 for failure.

EVP\_OpenFinal() returns 0 if the decrypt failed or 1 for success.

## SEE ALSO

evp(7), RAND\_bytes(3), EVP\_EncryptInit(3), EVP\_SealInit(3)

## COPYRIGHT

Copyright 2000-2020 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>>.