



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

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'EVP_PKEY_copy_parameters.3ossl' command

\$ man EVP_PKEY_copy_parameters.3ossl

EVP_PKEY_COPY_PARAMETERS(3ossl) OpenSSL EVP_PKEY_COPY_PARAMETERS(3ossl)

NAME

EVP_PKEY_missing_parameters, EVP_PKEY_copy_parameters,
EVP_PKEY_parameters_eq, EVP_PKEY_cmp_parameters, EVP_PKEY_eq,
EVP_PKEY_cmp - public key parameter and comparison functions

SYNOPSIS

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

```
int EVP_PKEY_missing_parameters(const EVP_PKEY *pkey);
```

```
int EVP_PKEY_copy_parameters(EVP_PKEY *to, const EVP_PKEY *from);
```

```
int EVP_PKEY_parameters_eq(const EVP_PKEY *a, const EVP_PKEY *b);
```

```
int EVP_PKEY_eq(const EVP_PKEY *a, const EVP_PKEY *b);
```

The following functions have been deprecated since OpenSSL 3.0, and can be hidden entirely by defining OPENSSL_API_COMPAT with a suitable version value, see openssl_user_macros(7):

```
int EVP_PKEY_cmp_parameters(const EVP_PKEY *a, const EVP_PKEY *b);
```

```
int EVP_PKEY_cmp(const EVP_PKEY *a, const EVP_PKEY *b);
```

DESCRIPTION

The function `EVP_PKEY_missing_parameters()` returns 1 if the public key parameters of `pkey` are missing and 0 if they are present or the algorithm doesn't use parameters.

The function `EVP_PKEY_copy_parameters()` copies the parameters from `key` from to `key to`. An error is returned if the parameters are missing in `from` or present in both `from` and `to` and mismatch. If the parameters in `from` and `to` are both present and match this function has no effect.

The function `EVP_PKEY_parameters_eq()` checks the parameters of keys `a` and `b` for equality.

The function `EVP_PKEY_eq()` checks the keys `a` and `b` for equality, including their parameters if they are available.

NOTES

The main purpose of the functions `EVP_PKEY_missing_parameters()` and `EVP_PKEY_copy_parameters()` is to handle public keys in certificates where the parameters are sometimes omitted from a public key if they are inherited from the CA that signed it.

The deprecated functions `EVP_PKEY_cmp()` and `EVP_PKEY_cmp_parameters()` differ in their return values compared to other `_cmp()` functions. They are aliases for `EVP_PKEY_eq()` and `EVP_PKEY_parameters_eq()`.

The function `EVP_PKEY_cmp()` previously only checked the key parameters (if there are any) and the public key, assuming that there always was a public key and that private key equality could be derived from that.

Because it's no longer assumed that the private key in an `EVP_PKEY(3)` is always accompanied by a public key, the comparison can not rely on public key comparison alone.

Instead, `EVP_PKEY_eq()` (and therefore also `EVP_PKEY_cmp()`) now compares:

1. the key parameters (if there are any)
2. the public keys or the private keys of the two `EVP_PKEY`s, depending on what they both contain.

RETURN VALUES

The function `EVP_PKEY_missing_parameters()` returns 1 if the public key parameters of `pkey` are missing and 0 if they are present or the algorithm doesn't use parameters.

These functions `EVP_PKEY_copy_parameters()` returns 1 for success and 0 for failure.

The functions `EVP_PKEY_cmp_parameters()`, `EVP_PKEY_parameters_eq()`, `EVP_PKEY_cmp()` and `EVP_PKEY_eq()` return 1 if their inputs match, 0 if they don't match, -1 if the key types are different and -2 if the operation is not supported.

SEE ALSO

`EVP_PKEY_CTX_new(3)`, `EVP_PKEY_keygen(3)`

HISTORY

The `EVP_PKEY_cmp()` and `EVP_PKEY_cmp_parameters()` functions were deprecated in OpenSSL 3.0.

The `EVP_PKEY_eq()` and `EVP_PKEY_parameters_eq()` were added in OpenSSL 3.0 to replace `EVP_PKEY_cmp()` and `EVP_PKEY_cmp_parameters()`.

COPYRIGHT

Copyright 2006-2021 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_PKEY_COPY_PARAMETERS(3openssl)