



## **Red Hat Enterprise Linux Release 9.2 Manual Pages on 'EVP\_KEYMGMT-EC.7oss1' command**

**\$ man EVP\_KEYMGMT-EC.7oss1**

EVP\_PKEY-EC(7oss1)            OpenSSL            EVP\_PKEY-EC(7oss1)

NAME

EVP\_PKEY-EC, EVP\_KEYMGMT-EC - EVP\_PKEY EC keytype and algorithm support

DESCRIPTION

The EC keytype is implemented in OpenSSL's default provider.

Common EC parameters

The normal way of specifying domain parameters for an EC curve is via the curve name "group". For curves with no curve name, explicit parameters can be used that specify "field-type", "p", "a", "b", "generator" and "order". Explicit parameters are supported for backwards compability reasons, but they are not compliant with multiple standards (including RFC5915) which only allow named curves.

The following KeyGen/Gettable/Import/Export types are available for the built-in EC algorithm:

"group" (OSSL\_PKEY\_PARAM\_GROUP\_NAME) <UTF8 string>

The curve name.

"field-type" (OSSL\_PKEY\_PARAM\_EC\_FIELD\_TYPE) <UTF8 string>

The value should be either "prime-field" or "characteristic-two-field", which correspond to prime field  $F_p$  and binary field  $F_{2^m}$ .

"p" (OSSL\_PKEY\_PARAM\_EC\_P) <unsigned integer>

For a curve over  $F_p$  p is the prime for the field. For a curve over  $F_{2^m}$  p represents the irreducible polynomial - each bit represents a term in the polynomial. Therefore, there will either be three or

five bits set dependent on whether the polynomial is a trinomial or a pentanomial.

"a" (OSSL\_PKEY\_PARAM\_EC\_A) <unsigned integer>

"b" (OSSL\_PKEY\_PARAM\_EC\_B) <unsigned integer>

"seed" (OSSL\_PKEY\_PARAM\_EC\_SEED) <octet string>

a and b represents the coefficients of the curve For  $F_p$ :  $y^2 \bmod p = x^3 + ax + b \bmod p$  OR For  $F_{2^m}$ :  $y^2 + xy = x^3 + ax^2 + b$

seed is an optional value that is for information purposes only.

It represents the random number seed used to generate the coefficient b from a random number.

"generator" (OSSL\_PKEY\_PARAM\_EC\_GENERATOR) <octet string>

"order" (OSSL\_PKEY\_PARAM\_EC\_ORDER) <unsigned integer>

"cofactor" (OSSL\_PKEY\_PARAM\_EC\_COFACTOR) <unsigned integer>

The generator is a well defined point on the curve chosen for cryptographic operations. The encoding conforms with Sec. 2.3.3 of the SECG SEC 1 ("Elliptic Curve Cryptography") standard. See EC\_POINT\_oct2point(). Integers used for point multiplications will be between 0 and order - 1. cofactor is an optional value. order multiplied by the cofactor gives the number of points on the curve.

"decoded-from-explicit"

(OSSL\_PKEY\_PARAM\_EC\_DECODED\_FROM\_EXPLICIT\_PARAMS) <integer>

Gets a flag indicating whether the key or parameters were decoded from explicit curve parameters. Set to 1 if so or 0 if a named curve was used.

"use-cofactor-flag" (OSSL\_PKEY\_PARAM\_USE\_COFACTOR\_ECDH) <integer>

Enable Cofactor DH (ECC CDH) if this value is 1, otherwise it uses normal EC DH if the value is zero. The cofactor variant multiplies the shared secret by the EC curve's cofactor (note for some curves the cofactor is 1).

"encoding" (OSSL\_PKEY\_PARAM\_EC\_ENCODING) <UTF8 string>

Set the format used for serializing the EC group parameters. Valid values are "explicit" or "named\_curve". The default value is

"named\_curve".

"point-format" (OSSL\_PKEY\_PARAM\_EC\_POINT\_CONVERSION\_FORMAT) <UTF8 string>

Sets or gets the point\_conversion\_form for the key. For a description of point\_conversion\_forms please see EC\_POINT\_new(3).

Valid values are "uncompressed" or "compressed". The default value is "uncompressed".

"group-check" (OSSL\_PKEY\_PARAM\_EC\_GROUP\_CHECK\_TYPE) <UTF8 string>

Sets or Gets the type of group check done when EVP\_PKEY\_param\_check() is called. Valid values are "default", "named" and "named-nist". The "named" type checks that the domain parameters match the inbuilt curve parameters, "named-nist" is similar but also checks that the named curve is a nist curve. The "default" type does domain parameter validation for the OpenSSL default provider, but is equivalent to "named-nist" for the OpenSSL FIPS provider.

"include-public" (OSSL\_PKEY\_PARAM\_EC\_INCLUDE\_PUBLIC) <integer>

Setting this value to 0 indicates that the public key should not be included when encoding the private key. The default value of 1 will include the public key.

See also EVP\_KEYEXCH-ECDH(7) for the related

OSSL\_EXCHANGE\_PARAM\_EC\_ECDH\_COFACTOR\_MODE parameter that can be set on a per-operation basis.

"pub" (OSSL\_PKEY\_PARAM\_PUB\_KEY) <octet string>

The public key value in encoded EC point format. This parameter is used when importing or exporting the public key value with the EVP\_PKEY\_fromdata() and EVP\_PKEY\_todata() functions.

"priv" (OSSL\_PKEY\_PARAM\_PRIV\_KEY) <unsigned integer>

The private key value.

"encoded-pub-key" (OSSL\_PKEY\_PARAM\_ENCODED\_PUBLIC\_KEY) <octet string>

Used for getting and setting the encoding of an EC public key. The public key is expected to be a point conforming to Sec. 2.3.4 of the SECG SEC 1 ("Elliptic Curve Cryptography") standard.

"qx" (OSSL\_PKEY\_PARAM\_EC\_PUB\_X) <unsigned integer>

Used for getting the EC public key X component.

"qy" (OSSL\_PKEY\_PARAM\_EC\_PUB\_Y) <unsigned integer>

Used for getting the EC public key Y component.

(OSSL\_PKEY\_PARAM\_DEFAULT\_DIGEST) <UTF8 string>

Getter that returns the default digest name. (Currently returns

"SHA256" as of OpenSSL 3.0).

The following Gettable types are also available for the built-in EC algorithm:

"basis-type" (OSSL\_PKEY\_PARAM\_EC\_CHAR2\_TYPE) <UTF8 string>

Supports the values "tpBasis" for a trinomial or "ppBasis" for a pentanomial. This field is only used for a binary field  $F_2^m$ .

"m" (OSSL\_PKEY\_PARAM\_EC\_CHAR2\_M) <integer>

"tp" (OSSL\_PKEY\_PARAM\_EC\_CHAR2\_TP\_BASIS) <integer>

"k1" (OSSL\_PKEY\_PARAM\_EC\_CHAR2\_PP\_K1) <integer>

"k2" (OSSL\_PKEY\_PARAM\_EC\_CHAR2\_PP\_K2) <integer>

"k3" (OSSL\_PKEY\_PARAM\_EC\_CHAR2\_PP\_K3) <integer>

These fields are only used for a binary field  $F_2^m$ .  $m$  is the degree of the binary field.

$tp$  is the middle bit of a trinomial so its value must be in the range  $m > tp > 0$ .

$k_1$ ,  $k_2$  and  $k_3$  are used to get the middle bits of a pentanomial such that  $m > k_3 > k_2 > k_1 > 0$

#### EC key validation

For EC keys, `EVP_PKEY_param_check(3)` behaves in the following way: For the OpenSSL default provider it uses either `EC_GROUP_check(3)` or `EC_GROUP_check_named_curve(3)` depending on the flag `EC_FLAG_CHECK_NAMED_GROUP`. The OpenSSL FIPS provider uses `EC_GROUP_check_named_curve(3)` in order to conform to SP800-56Ar3 Assurances of Domain-Parameter Validity.

For EC keys, `EVP_PKEY_param_check_quick(3)` is equivalent to `EVP_PKEY_param_check(3)`.

For EC keys, `EVP_PKEY_public_check(3)` and `EVP_PKEY_public_check_quick(3)` conform to SP800-56Ar3 ECC Full Public-

Key Validation and ECC Partial Public-Key Validation respectively.

For EC Keys, EVP\_PKEY\_private\_check(3) and EVP\_PKEY\_pairwise\_check(3) conform to SP800-56Ar3 Private key validity and Owner Assurance of Pair-wise Consistency respectively.

## EXAMPLES

An EVP\_PKEY context can be obtained by calling:

```
EVP_PKEY_CTX *pctx =  
    EVP_PKEY_CTX_new_from_name(NULL, "EC", NULL);
```

An EVP\_PKEY ECDSA or ECDH key can be generated with a "P-256" named group by calling:

```
pkey = EVP_EC_gen("P-256");
```

or like this:

```
EVP_PKEY *key = NULL;  
OSSL_PARAM params[2];  
EVP_PKEY_CTX *gctx =  
    EVP_PKEY_CTX_new_from_name(NULL, "EC", NULL);  
EVP_PKEY_keygen_init(gctx);  
params[0] = OSSL_PARAM_construct_utf8_string(OSSL_PKEY_PARAM_GROUP_NAME,  
                                             "P-256", 0);  
params[1] = OSSL_PARAM_construct_end();  
EVP_PKEY_CTX_set_params(gctx, params);  
EVP_PKEY_generate(gctx, &key);  
EVP_PKEY_print_private(bio_out, key, 0, NULL);  
...  
EVP_PKEY_free(key);  
EVP_PKEY_CTX_free(gctx);
```

An EVP\_PKEY EC CDH (Cofactor Diffie-Hellman) key can be generated with a "K-571" named group by calling:

```
int use_cdh = 1;  
EVP_PKEY *key = NULL;  
OSSL_PARAM params[3];  
EVP_PKEY_CTX *gctx =  
    EVP_PKEY_CTX_new_from_name(NULL, "EC", NULL);
```

```

EVP_PKEY_keygen_init(gctx);

params[0] = OSSL_PARAM_construct_utf8_string(OSSL_PKEY_PARAM_GROUP_NAME,
                                             "K-571", 0);

/*
 * This curve has a cofactor that is not 1 - so setting CDH mode changes
 * the behaviour. For many curves the cofactor is 1 - so setting this has
 * no effect.
 */

params[1] = OSSL_PARAM_construct_int(OSSL_PKEY_PARAM_USE_COFACTOR_ECDH,
                                     &use_cdh);

params[2] = OSSL_PARAM_construct_end();
EVP_PKEY_CTX_set_params(gctx, params);
EVP_PKEY_generate(gctx, &key);
EVP_PKEY_print_private(bio_out, key, 0, NULL);

...

EVP_PKEY_free(key);
EVP_PKEY_CTX_free(gctx);

```

#### SEE ALSO

[EVP\\_EC\\_gen\(3\)](#), [EVP\\_KEYMGMT\(3\)](#), [EVP\\_PKEY\(3\)](#), [provider-keymgmt\(7\)](#),  
[EVP\\_SIGNATURE-ECDSA\(7\)](#), [EVP\\_KEYEXCH-ECDH\(7\)](#)

#### COPYRIGHT

Copyright 2020-2022 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-EC(7openssl)