



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 'EC_GFp_mont_method.3ossl'

\$ man EC_GFp_mont_method.3ossl

EC_GFP_SIMPLE_METHOD(3ossl) OpenSSL EC_GFP_SIMPLE_METHOD(3ossl)

NAME

EC_GFp_simple_method, EC_GFp_mont_method, EC_GFp_nist_method,
EC_GFp_nistp224_method, EC_GFp_nistp256_method, EC_GFp_nistp521_method,
EC_GF2m_simple_method, EC_METHOD_get_field_type - Functions for
obtaining EC_METHOD objects

SYNOPSIS

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

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):

```
const EC_METHOD *EC_GFp_simple_method(void);  
const EC_METHOD *EC_GFp_mont_method(void);  
const EC_METHOD *EC_GFp_nist_method(void);
```

```
const EC_METHOD *EC_GFp_nistp224_method(void);
const EC_METHOD *EC_GFp_nistp256_method(void);
const EC_METHOD *EC_GFp_nistp521_method(void);

const EC_METHOD *EC_GF2m_simple_method(void);

int EC_METHOD_get_field_type(const EC_METHOD *meth);
```

DESCRIPTION

All const EC_METHOD *EC_GF* functions were deprecated in OpenSSL 3.0, since EC_METHOD is no longer a public concept.

The Elliptic Curve library provides a number of different implementations through a single common interface. When constructing a curve using EC_GROUP_new (see EC_GROUP_new(3)) an implementation method must be provided. The functions described here all return a const pointer to an EC_METHOD structure that can be passed to EC_GROUP_NEW. It is important that the correct implementation type for the form of curve selected is used.

For F_2^m curves there is only one implementation choice, i.e. EC_GF2_simple_method.

For F_p curves the lowest common denominator implementation is the EC_GFp_simple_method implementation. All other implementations are based on this one. EC_GFp_mont_method builds on EC_GFp_simple_method but adds the use of montgomery multiplication (see BN_mod_mul_montgomery(3)). EC_GFp_nist_method offers an implementation optimised for use with NIST recommended curves (NIST curves are available through EC_GROUP_new_by_curve_name as described in EC_GROUP_new(3)).

The functions EC_GFp_nistp224_method, EC_GFp_nistp256_method and

EC_GFp_nistp521_method offer 64 bit optimised implementations for the NIST P224, P256 and P521 curves respectively. Note, however, that these implementations are not available on all platforms.

EC_METHOD_get_field_type() was deprecated in OpenSSL 3.0. Applications should use EC_GROUP_get_field_type() as a replacement (see EC_GROUP_copy(3)).

RETURN VALUES

All EC_GFp* functions and EC_GF2m_simple_method always return a const pointer to an EC_METHOD structure.

EC_METHOD_get_field_type returns an integer that identifies the type of field the EC_METHOD structure supports.

SEE ALSO

crypto(7), EC_GROUP_new(3), EC_GROUP_copy(3), EC_POINT_new(3), EC_POINT_add(3), EC_KEY_new(3), d2i_ECPKParameters(3), BN_mod_mul_montgomery(3)

HISTORY

EC_GFp_simple_method(), EC_GFp_mont_method(void), EC_GFp_nist_method(), EC_GFp_nistp224_method(), EC_GFp_nistp256_method(), EC_GFp_nistp521_method(), EC_GF2m_simple_method(), and EC_METHOD_get_field_type() were deprecated in OpenSSL 3.0.

COPYRIGHT

Copyright 2013-2021 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 EC_GFP_SIMPLE_METHOD(3ossil)