



*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\_nist\_method.3ossl'***

***\$ man EC\_GFp\_nist\_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)