

**NAME**

openssl-ecparam - EC parameter manipulation and generation

**SYNOPSIS**

```
openssl ecparam [-help] [-inform DER|PEM] [-outform DER|PEM] [-in filename] [-out filename]
[-noout] [-text] [-check] [-check_named] [-name arg] [-list_curves] [-conv_form arg] [-param_enc arg]
[-no_seed] [-genkey] [-engine id] [-rand files] [-writerand file] [-provider name] [-provider-path path]
[-propquery propq]
```

**DESCRIPTION**

This command is used to manipulate or generate EC parameter files.

OpenSSL is currently not able to generate new groups and therefore this command can only create EC parameters from known (named) curves.

**OPTIONS****-help**

Print out a usage message.

**-inform DER|PEM**

The EC parameters input format; unspecified by default. See **openssl-format-options(1)** for details.

**-outform DER|PEM**

The EC parameters output format; the default is **PEM**. See **openssl-format-options(1)** for details.

Parameters are encoded as **EcpkParameters** as specified in IETF RFC 3279.

**-in filename**

This specifies the input filename to read parameters from or standard input if this option is not specified.

**-out filename**

This specifies the output filename parameters to. Standard output is used if this option is not present. The output filename should **not** be the same as the input filename.

**-noout**

This option inhibits the output of the encoded version of the parameters.

**-text**

This option prints out the EC parameters in human readable form.

**-check**

Validate the elliptic curve parameters.

**-check\_named**

Validate the elliptic name curve parameters by checking if the curve parameters match any built-in curves.

**-name *arg***

Use the EC parameters with the specified 'short' name. Use **-list\_curves** to get a list of all currently implemented EC parameters.

**-list\_curves**

Print out a list of all currently implemented EC parameters names and exit.

**-conv\_form *arg***

This specifies how the points on the elliptic curve are converted into octet strings. Possible values are: **compressed**, **uncompressed** (the default value) and **hybrid**. For more information regarding the point conversion forms please read the X9.62 standard. **Note** Due to patent issues the **compressed** option is disabled by default for binary curves and can be enabled by defining the preprocessor macro **OPENSSL\_EC\_BIN\_PT\_COMP** at compile time.

**-param\_enc *arg***

This specifies how the elliptic curve parameters are encoded. Possible value are: **named\_curve**, i.e. the ec parameters are specified by an OID, or **explicit** where the ec parameters are explicitly given (see RFC 3279 for the definition of the EC parameters structures). The default value is **named\_curve**. **Note** the **implicitlyCA** alternative, as specified in RFC 3279, is currently not implemented in OpenSSL.

**-no\_seed**

This option inhibits that the 'seed' for the parameter generation is included in the ECParameters structure (see RFC 3279).

**-genkey**

This option will generate an EC private key using the specified parameters.

**-engine *id***

See "Engine Options" in **openssl(1)**. This option is deprecated.

**-rand** *files*, **-writerand** *file*

See "Random State Options" in **openssl(1)** for details.

**-provider** *name*

**-provider-path** *path*

**-propquery** *propq*

See "Provider Options" in **openssl(1)**, **provider(7)**, and **property(7)**.

The **openssl-genpkey(1)** and **openssl-pkeyparam(1)** commands are capable of performing all the operations this command can, as well as supporting other public key types.

## EXAMPLES

The documentation for the **openssl-genpkey(1)** and **openssl-pkeyparam(1)** commands contains examples equivalent to the ones listed here.

To create EC parameters with the group 'prime192v1':

```
openssl ecparam -out ec_param.pem -name prime192v1
```

To create EC parameters with explicit parameters:

```
openssl ecparam -out ec_param.pem -name prime192v1 -param_enc explicit
```

To validate given EC parameters:

```
openssl ecparam -in ec_param.pem -check
```

To create EC parameters and a private key:

```
openssl ecparam -out ec_key.pem -name prime192v1 -genkey
```

To change the point encoding to 'compressed':

```
openssl ecparam -in ec_in.pem -out ec_out.pem -conv_form compressed
```

To print out the EC parameters to standard output:

```
openssl ecparam -in ec_param.pem -noout -text
```

## SEE ALSO

**openssl(1), openssl-pkeyparam(1), openssl-genpkey(1), openssl-ec(1), openssl-dsaparam(1)**

## HISTORY

The **-engine** option was deprecated in OpenSSL 3.0.

The **-C** option was removed in OpenSSL 3.0.

## COPYRIGHT

Copyright 2003-2021 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>.