NAME

ecparam - EC parameter manipulation and generation

SYNOPSIS

openssl ecparam [**-inform DER|PEM**] [**-outform DER|PEM**] [**-in filename**] [**-out filename**] [**-noout**] [**-text**] [**-C**] [**-check**] [**-name arg**] [**-list_curves**] [**-conv_form arg**] [**-param_enc arg**] [**-no_seed**] [**-rand file(s)**] [**-genkey**] [**-engine id**]

DESCRIPTION

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

OPTIONS

-inform DER|PEM

This specifies the input format. The **DER** option uses an ASN.1 DER encoded form compatible with RFC 3279 EcpkParameters. The PEM form is the default format: it consists of the **DER** format base64 encoded with additional header and footer lines.

-outform DER|PEM

This specifies the output format, the options have the same meaning as the **-inform** option.

-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.

-C This option converts the EC parameters into C code. The parameters can then be loaded by calling the ***get_ec_group_XXX()*** function.

-check

Validate the elliptic curve parameters.

-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

If this options is specified **ecparam** will print out a list of all currently implemented EC parameters names and exit.

-conv_form

This specifies how the points on the elliptic curve are converted into octet strings. Possible values are: **compressed** (the default value), **uncompressed** 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 a 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 a EC private key using the specified parameters.

-rand file(s)
a file or files containing random data used to seed the random number generator, or an EGD socket (see *RAND_egd(3)*). Multiple files can be specified separated by a OS-dependent character. The separator is**;** for MS-Windo ws, **,** for OpenVMS, and **:** for all others.

-engine id
specifying an engine (by its unique **id** string) will cause **ecparam** to attempt to obtain a functional reference to the specified engine, thus initialising it if needed. The engine will then be set as the default for all available algorithms.

NOTES

PEM format EC parameters use the header and footer lines:

```
-----BEGIN EC PARAMETERS-----
-----END EC PARAMETERS-----
```

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

EXAMPLES

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

ec(1), *dsaparam(1)*

HISTORY

The ecparam command was first introduced in OpenSSL 0.9.8.

AUTHOR

Nils Larsch for the OpenSSL project (http://www.openssl.org)