NAME

SSL_CTX_set1_curves, SSL_CTX_set1_curves_list, SSL_set1_curves, SSL_set1_curves_list, SSL_get1_curves, SSL_get_shared_curve - EC supported curve functions

SYNOPSIS

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

int SSL_CTX_set1_curves(SSL_CTX *ctx, int *clist, int clistlen);
int SSL_CTX_set1_curves_list(SSL_CTX *ctx, char *list);

int SSL_set1_curves(SSL *ssl, int *clist, int clistlen);
int SSL_set1_curves_list(SSL *ssl, char *list);

int SSL_get1_curves(SSL *ssl, int *curves);
int SSL_get_shared_curve(SSL *s, int n);
```

DESCRIPTION

SSL_CTX_set1_curves() sets the supported curves for **ctx** to **clistlen** curves in the array **clist**. The array consist of all NIDs of curves in preference order. For a TLS client the curves are used directly in the supported curves extension. For a TLS server the curves are used to determine the set of shared curves.

SSL_CTX_set1_curves_list() sets the supported curves for **ctx** to string **list**. The string is a colon separated list of curve NIDs or names, for example ‘‘P-521:P-384:P-256’’.

SSL_set1_curves() and *SSL_set1_curves_list()* are similar except they set supported curves for the SSL structure **ssl**.

SSL_get1_curves() returns the set of supported curves sent by a client in the supported curves extension. It returns the total number of supported curves. The **curves** parameter can be **NULL** to simply return the number of curves for memory allocation purposes. The **curves** array is in the form of a set of curve NIDs in preference order. It can return zero if the client did not send a supported curves extension.

SSL_get_shared_curve() returns shared curve **n** for a server-side SSL **ssl**. If **n** is -1 then the total number of shared curves is returned, which may be zero. Other than for diagnostic purposes, most applications will only be interested in the first shared curve so **n** is normally set to zero. If the value **n** is out of range, NID_undef is returned.

All these functions are implemented as macros.

NOTES

If an application wishes to make use of several of these functions for configuration purposes either on a command line or in a file it should consider using the SSL_CONF interface instead of manually parsing options.

RETURN VALUES

SSL_CTX_set1_curves(), *SSL_CTX_set1_curves_list()*, *SSL_set1_curves()* and *SSL_set1_curves_list()*, return 1 for success and 0 for failure.

SSL_get1_curves() returns the number of curves, which may be zero.

SSL_get_shared_curve() returns the NID of shared curve **n** or NID_undef if there is no shared curve **n**; or the total number of shared curves if **n** is -1.

When called on a client **ssl**, *SSL_get_shared_curve()* has no meaning and returns -1.

SEE ALSO

SSL_CTX_add_extra_chain_cert(3)

HISTORY

These functions were first added to OpenSSL 1.0.2.

COPYRIGHT