NAME

DH_generate_parameters_ex, DH_generate_parameters, DH_check - generate and check Diffie-Hellman parameters

SYNOPSIS

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

int DH_generate_parameters_ex(DH *dh, int prime_len,int generator, BN_GENCB *cb);

int DH_check(DH *dh, int *codes);
```

Deprecated:

```
DH *DH_generate_parameters(int prime_len, int generator,
void (*callback)(int, int, void *), void *cb_arg);
```

DESCRIPTION

DH_generate_parameters_ex() generates Diffie-Hellman parameters that can be shared among a group of users, and stores them in the provided **DH** structure. The pseudo-random number generator must be seeded prior to calling *DH_generate_parameters()*.

prime_len is the length in bits of the safe prime to be generated. **generator** is a small number > 1, typically 2 or 5.

A callback function may be used to provide feedback about the progress of the key generation. If **cb** is not **NULL**, it will be called as described in *BN_generate_prime(3)* while a random prime number is generated, and when a prime has been found, **BN_GENCB_call(cb, 3, 0)**is called. See *BN_generate_prime(3)* for information on the*BN_GENCB_c all()* function.

DH_check() validates Diffie-Hellman parameters. It checks that **p** is a safe prime, and that **g** is a suitable generator. In the case of an error, the bit flags DH_CHECK_P_NOT_SAFE_PRIME or DH_NOT_SUITABLE_GENERATOR are set in ***codes**. DH_UNABLE_TO_CHECK_GENERATOR is set if the generator cannot be checked, i.e. it does not equal 2 or 5.

RETURN VALUES

DH_generate_parameters_ex() and *DH_check()* return 1 if the check could be performed, 0 otherwise.

DH_generate_parameters() (deprecated) returns a pointer to the DH structure, or NULL if the parameter generation fails.

The error codes can be obtained by *ERR_get_error(3)*.

NOTES

DH_generate_parameters_ex() and *DH_generate_parameters()* may run for several hours before finding a suitable prime.

The parameters generated by *DH_generate_parameters_ex()* and *DH_generate_parameters()* are not to be used in signature schemes.

BUGS

If **generator** is not 2 or 5, **dh->g=generator** is not a usable generator.

SEE ALSO

dh(3), *ERR_get_error(3)*, *rand(3)*, *DH_free(3)*

HISTORY

DH_check() is available in all versions of SSLeay and OpenSSL. The **cb_arg** argument to *DH_generate_parameters()* was added in SSLeay 0.9.0.

In versions before OpenSSL 0.9.5, DH_CHECK_P_NOT_STRONG_PRIME is used instead of DH_CHECK_P_NOT_SAFE_PRIME.