NAME

DH_set_default_method, DH_get_default_method, DH_set_method, DH_new_method, DH_OpenSSL - select DH method

SYNOPSIS

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

void DH_set_default_method(const DH_METHOD *meth);

const DH_METHOD *DH_get_default_method(void);

int DH_set_method(DH *dh, const DH_METHOD *meth);

DH *DH_new_method(ENGINE *engine);

const DH_METHOD *DH_OpenSSL(void);
```

DESCRIPTION

A **DH_METHOD** specifies the functions that OpenSSL uses for Diffie-Hellman operations. By modifying the method, alternative implementations such as hardware accelerators may be used. IMPORTANT: See the NOTES section for important information about how these DH API functions are affected by the use of **ENGINE** API calls.

Initially, the default DH_METHOD is the OpenSSL internal implementation, as returned by *DH_OpenSSL()*.

DH_set_default_method() makes **meth** the default method for all DH structures created later. **NB**: This is true only whilst no ENGINE has been set as a default for DH, so this function is no longer recommended.

DH_get_default_method() returns a pointer to the current default DH_METHOD. However, the meaningfulness of this result is dependent on whether the ENGINE API is being used, so this function is no longer recommended.

DH_set_method() selects **meth** to perform all operations using the key **dh**. This will replace the DH_METHOD used by the DH key and if the previous method was supplied by an ENGINE, the handle to that ENGINE will be released during the change. It is possible to have DH keys that only work with certain DH_METHOD implementations (eg. from an ENGINE module that supports embedded hardware-protected keys), and in such cases attempting to change the DH_METHOD for the key can have unexpected results.

DH_new_method() allocates and initializes a DH structure so that **engine** will be used for the DH operations. If **engine** is NULL, the default ENGINE for DH operations is used, and if no default ENGINE is set, the DH_METHOD controlled by *DH_set_default_method()* is used.

THE DH_METHOD STRUCTURE

```
typedef struct dh_meth_st
{
/* name of the implementation */
const char *name;

/* generate private and public DH values for key agreement */
int (*generate_key)(DH *dh);

/* compute shared secret */
int (*compute_key)(unsigned char *key, BIGNUM *pub_key, DH *dh);

/* compute r = a  p mod m (May be NULL for some implementations) */
```

```
int (*bn_mod_exp)(DH *dh, BIGNUM *r, BIGNUM *a, const BIGNUM *p,
const BIGNUM *m, BN_CTX *ctx,
BN_MONT_CTX *m_ctx);

/* called at DH_new */
int (*init)(DH *dh);

/* called at DH_free */
int (*finish)(DH *dh);

int flags;

char *app_data; /* ?? */

} DH_METHOD;
```

RETURN VALUES

DH_OpenSSL() and *DH_get_default_method()* return pointers to the respective **DH_METHOD**s.

DH_set_default_method() returns no value.

DH_set_method() returns non-zero if the provided **meth** was successfully set as the method for **dh** (including unloading the ENGINE handle if the previous method was supplied by an ENGINE).

DH_new_method() returns NULL and sets an error code that can be obtained by *ERR_get_error(3)* if the allocation fails. Otherwise it returns a pointer to the newly allocated structure.

NOTES

As of version 0.9.7, DH_METHOD implementations are grouped together with other algorithmic APIs (eg. RSA_METHOD, EVP_CIPHER, etc) in **ENGINE** modules. If a default ENGINE is specified for DH functionality using an ENGINE API function, that will override any DH defaults set using the DH API (ie. *DH_set_default_metho d()*). For this reason, the ENGINE API is the recommended way to control default implementations for use in DH and other cryptographic algorithms.

SEE ALSO

dh(3), *DH_new(3)*

HISTORY

DH_set_default_method(), *DH_get_default_method()*, *DH_set_method()*, *DH_new_method()* and *DH_OpenSSL()* were added in OpenSSL 0.9.4.

DH_set_default_openssl_method() and *DH_get_default_openssl_method()* replaced *DH_set_default_method()* and *DH_get_default_method()* respectively, and *DH_set_method()* and *DH_new_method()* were altered to use **ENGINE**s rather than **DH_METHOD**s during development of the engine version of OpenSSL 0.9.6. For 0.9.7, the handling of defaults in the ENGINE API was restructured so that this change was reversed, and behaviour of the other functions resembled more closely the previous behaviour. The behaviour of defaults in the ENGINE API now transparently overrides the behaviour of defaults in the DH API without requiring changing these function prototypes.