NAME

DSA_set_default_method, DSA_get_default_method, DSA_set_method, DSA_new_method, DSA_OpenSSL - select DSA method

SYNOPSIS

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

void DSA_set_default_method(const DSA_METHOD *meth);

const DSA_METHOD *DSA_get_default_method(void);

int DSA_set_method(DSA *dsa, const DSA_METHOD *meth);

DSA *DSA_new_method(ENGINE *engine);

DSA_METHOD *DSA_OpenSSL(void);
```

DESCRIPTION

A **DSA_METHOD** specifies the functions that OpenSSL uses for DSA 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 DSA API functions are affected by the use of **ENGINE** API calls.

Initially, the default DSA_METHOD is the OpenSSL internal implementation, as returned by *DSA_OpenSSL()*.

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

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

DSA_set_method() selects **meth** to perform all operations using the key **rsa**. This will replace the DSA_METHOD used by the DSA 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 DSA keys that only work with certain DSA_METHOD implementations (eg. from an ENGINE module that supports embedded hardware-protected keys), and in such cases attempting to change the DSA_METHOD for the key can have unexpected results.

DSA_new_method() allocates and initializes a DSA structure so that **engine** will be used for the DSA operations. If **engine** is NULL, the default engine for DSA operations is used, and if no default ENGINE is set, the DSA_METHOD controlled by *DSA_set_default_method()* is used.

THE DSA_METHOD STRUCTURE

struct { /* name of the implementation */ const char *name;

```
/* sign */
DSA_SIG *(*dsa_do_sign)(const unsigned char *dgst, int dlen,
DSA *dsa);

/* pre-compute k-1 and r */
int (*dsa_sign_setup)(DSA *dsa, BN_CTX *ctx_in, BIGNUM **kinvp,
BIGNUM **rp);

/* verify */
int (*dsa_do_verify)(const unsigned char *dgst, int dgst_len,
DSA_SIG *sig, DSA *dsa);
```

```
/* compute rr = a1p1 * a2p2 mod m (May be NULL for some
implementations) */
int (*dsa_mod_exp)(DSA *dsa, BIGNUM *rr, BIGNUM *a1, BIGNUM *p1,
BIGNUM *a2, BIGNUM *p2, BIGNUM *m,
BN_CTX *ctx, BN_MONT_CTX *in_mont);

/* compute r = a  p mod m (May be NULL for some implementations) */
int (*bn_mod_exp)(DSA *dsa, BIGNUM *r, BIGNUM *a,
const BIGNUM *p, const BIGNUM *m,
BN_CTX *ctx, BN_MONT_CTX *m_ctx);

/* called at DSA_new */
int (*init)(DSA *DSA);

/* called at DSA_free */
int (*finish)(DSA *DSA);

int flags;

char *app_data; /* ?? */

} DSA_METHOD;
```

RETURN VALUES

DSA_OpenSSL() and *DSA_get_default_method()* return pointers to the respective **DSA_METHOD**s.

DSA_set_default_method() returns no value.

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

DSA_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, DSA_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 DSA functionality using an ENGINE API function, that will override any DSA defaults set using the DSA API (ie. *DSA_set_default_metho d()*). For this reason, the ENGINE API is the recommended way to control default implementations for use in DSA and other cryptographic algorithms.

SEE ALSO

dsa(3), *DSA_new(3)*

HISTORY

DSA_set_default_method(), *DSA_get_default_method()*, *DSA_set_method()*, *DSA_new_method()* and *DSA_OpenSSL()* were added in OpenSSL 0.9.4.

DSA_set_default_openssl_method() and *DSA_get_default_openssl_method()* replaced *DSA_set_default_method()* and *DSA_get_default_method()* respectively, and *DSA_set_method()* and *DSA_new_method()* were altered to use **ENGINE**s rather than **DSA_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 DSA API without requiring changing these function prototypes.