

**NAME**

DSA\_sign, DSA\_sign\_setup, DSA\_verify - DSA signatures

**SYNOPSIS**

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

```
int DSA_sign(int type, const unsigned char *dgst, int len,
             unsigned char *sigret, unsigned int *siglen, DSA *dsa);
```

```
int DSA_sign_setup(DSA *dsa, BN_CTX *ctx, BIGNUM **kinvp,
                  BIGNUM **r);
```

```
int DSA_verify(int type, const unsigned char *dgst, int len,
              unsigned char *sigbuf, int siglen, DSA *dsa);
```

**DESCRIPTION**

*DSA\_sign()* computes a digital signature on the **len** byte message digest **dgst** using the private key **dsa** and places its ASN.1 DER encoding at **sigret**. The length of the signature is places in **\*siglen**. **sigret** must point to *DSA\_size(dsa)* bytes of memory.

*DSA\_sign\_setup()* may be used to precompute part of the signing operation in case signature generation is time-critical. It expects **dsa** to contain DSA parameters. It places the precomputed values in newly allocated **BIGNUM**s at **\*kinvp** and **\*rp**, after freeing the old ones unless **\*kinvp** and **\*rp** are NULL. These values may be passed to *DSA\_sign()* in **dsa->kinv** and **dsa->r**. **ctx** is a pre-allocated **BN\_CTX** or NULL.

*DSA\_verify()* verifies that the signature **sigbuf** of size **siglen** matches a given message digest **dgst** of size **len**. **dsa** is the signer's public key.

The **type** parameter is ignored.

The PRNG must be seeded before *DSA\_sign()* (or *DSA\_sign\_setup()*) is called.

**RETURN VALUES**

*DSA\_sign()* and *DSA\_sign\_setup()* return 1 on success, 0 on error. *DSA\_verify()* returns 1 for a valid signature, 0 for an incorrect signature and -1 on error. The error codes can be obtained by [ERR\\_get\\_error\(3\)](#).

**CONFORMING TO**

US Federal Information Processing Standard FIPS 186 (Digital Signature Standard, DSS), ANSI X9.30

**SEE ALSO**

[dsa\(3\)](#), [ERR\\_get\\_error\(3\)](#), [rand\(3\)](#), [DSA\\_do\\_sign\(3\)](#)

**HISTORY**

*DSA\_sign()* and *DSA\_verify()* are available in all versions of SSLeay. *DSA\_sign\_setup()* was added in SSLeay 0.8.