NAME

DSA_do_sign, DSA_do_verify - raw DSA signature operations

SYNOPSIS

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

DSA_SIG *DSA_do_sign(const unsigned char *dgst, int dlen, DSA *dsa);

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

DESCRIPTION

DSA_do_sign() computes a digital signature on the **len** byte message digest **dgst** using the private key **dsa** and returns it in a newly allocated **DSA_SIG** structure.

DSA_sign_setup(3) may be used to precompute part of the signing operation in case signature generation is time-critical.

DSA_do_verify() verifies that the signature **sig** matches a given message digest **dgst** of size **len**. **dsa** is the signer's public key.

RETURN VALUES

DSA_do_sign() returns the signature, NULL on error. *DSA_do_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)*.

SEE ALSO

dsa(3), *ERR_get_error(3)*, *rand(3)*, *DSA_SIG_new(3)*, *DSA_sign(3)*

HISTORY

DSA_do_sign() and *DSA_do_verify()* were added in OpenSSL 0.9.3.