

NAME

DSA_dup_DH - create a DH structure out of DSA structure

SYNOPSIS

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

```
DH * DSA_dup_DH(const DSA *r);
```

DESCRIPTION

DSA_dup_DH() duplicates DSA parameters/keys as DH parameters/keys. *q* is lost during that conversion, but the resulting DH parameters contain its length.

RETURN VALUE

DSA_dup_DH() returns the new **DH** structure, and **NULL** on error. The error codes can be obtained by *ERR_get_error(3)*.

NOTE

Be careful to avoid small subgroup attacks when using this.

SEE ALSO

dh(3), *dsa(3)*, *ERR_get_error(3)*

HISTORY

DSA_dup_DH() was added in OpenSSL 0.9.4.