



Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'DSA_dup_DH.3oss1' command

\$ man DSA_dup_DH.3oss1

DSA_DUP_DH(3oss1) OpenSSL DSA_DUP_DH(3oss1)

NAME

DSA_dup_DH - create a DH structure out of DSA structure

SYNOPSIS

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

The following functions have been deprecated since OpenSSL 3.0, and can be hidden entirely by defining OPENSSL_API_COMPAT with a suitable version value, see openssl_user_macros(7):

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

DESCRIPTION

The function described on this page is deprecated. There is no direct replacement, applications should use the EVP_PKEY APIs for Diffie-Hellman operations.

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 VALUES

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_new(3), DSA_new(3), ERR_get_error(3)

HISTORY

This function was deprecated in OpenSSL 3.0.

COPYRIGHT

Copyright 2000-2021 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the "License"). You may not use

this file except in compliance with the License. You can obtain a copy

in the file LICENSE in the source distribution or at

<<https://www.openssl.org/source/license.html>>.

3.0.7

2023-07-13

DSA_DUP_DH(3ossl)