



*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 'DH\_compute\_key\_padded.3oss1' command**

***\$ man DH\_compute\_key\_padded.3oss1***

DH\_GENERATE\_KEY(3oss1)      OpenSSL      DH\_GENERATE\_KEY(3oss1)

### NAME

DH\_generate\_key, DH\_compute\_key, DH\_compute\_key\_padded - perform Diffie-Hellman key exchange

### SYNOPSIS

```
#include <openssl/dh.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):

```
int DH_generate_key(DH *dh);
```

```
int DH_compute_key(unsigned char *key, const BIGNUM *pub_key, DH *dh);
```

```
int DH_compute_key_padded(unsigned char *key, const BIGNUM *pub_key, DH *dh);
```

### DESCRIPTION

All of the functions described on this page are deprecated.

Applications should instead use EVP\_PKEY\_derive\_init(3) and EVP\_PKEY\_derive(3).

DH\_generate\_key() performs the first step of a Diffie-Hellman key exchange by generating private and public DH values. By calling DH\_compute\_key() or DH\_compute\_key\_padded(), these are combined with the other party's public value to compute the shared key.

DH\_generate\_key() expects dh to contain the shared parameters dh->p and dh->g. It generates a random private DH value unless dh->priv\_key is already set, and computes the corresponding public value dh->pub\_key,

which can then be published.

`DH_compute_key()` computes the shared secret from the private DH value in `dh` and the other party's public value in `pub_key` and stores it in `key`. `key` must point to `DH_size(dh)` bytes of memory. The padding style is RFC 5246 (8.1.2) that strips leading zero bytes. It is not constant time due to the leading zero bytes being stripped. The return value should be considered public.

`DH_compute_key_padded()` is similar but stores a fixed number of bytes. The padding style is NIST SP 800-56A (C.1) that retains leading zero bytes. It is constant time due to the leading zero bytes being retained. The return value should be considered public.

## RETURN VALUES

`DH_generate_key()` returns 1 on success, 0 otherwise.

`DH_compute_key()` returns the size of the shared secret on success, -1 on error.

`DH_compute_key_padded()` returns `DH_size(dh)` on success, -1 on error.

The error codes can be obtained by `ERR_get_error(3)`.

## SEE ALSO

`EVP_PKEY_derive(3)`, `DH_new(3)`, `ERR_get_error(3)`, `RAND_bytes(3)`,

`DH_size(3)`

## HISTORY

`DH_compute_key_padded()` was added in OpenSSL 1.0.2.

All of these functions were 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>](https://www.openssl.org/source/license.html).

3.0.7                    2023-07-13            `DH_GENERATE_KEY(3openssl)`