

NAME

DSA_generate_key – generate DSA key pair

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):

```
int DSA_generate_key(DSA *a);
```

DESCRIPTION

All of the functions described on this page are deprecated. Applications should instead use **EVP_PKEY_keygen_init** (3) and **EVP_PKEY_keygen** (3) as described in **EVP_PKEY-DSA** (7).

DSA_generate_key() expects **a** to contain DSA parameters. It generates a new key pair and stores it in **a->pub_key** and **a->priv_key**.

The random generator must be seeded prior to calling **DSA_generate_key()**. If the automatic seeding or reseeding of the OpenSSL CSPRNG fails due to external circumstances (see **RAND** (7)), the operation will fail.

RETURN VALUES

DSA_generate_key() returns 1 on success, 0 otherwise. The error codes can be obtained by **ERR_get_error** (3).

SEE ALSO

DSA_new (3), **ERR_get_error** (3), **RAND_bytes** (3), **DSA_generate_parameters_ex** (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>>.