

## NAME

`EVP_PKEY_get_default_digest_nid` – get default signature digest

## SYNOPSIS

```
#include <openssl/evp.h>
int EVP_PKEY_get_default_digest_nid(EVP_PKEY *pkey, int *pnid);
```

## DESCRIPTION

The `EVP_PKEY_get_default_digest_nid()` function sets `pnid` to the default message digest NID for the public key signature operations associated with key `pkey`. Note that some signature algorithms (i.e. Ed25519 and Ed448) do not use a digest during signing. In this case `pnid` will be set to `NID_undef`.

## NOTES

For all current standard OpenSSL public key algorithms SHA1 is returned.

## RETURN VALUES

The `EVP_PKEY_get_default_digest_nid()` function returns 1 if the message digest is advisory (that is other digests can be used) and 2 if it is mandatory (other digests can not be used). It returns 0 or a negative value for failure. In particular a return value of -2 indicates the operation is not supported by the public key algorithm.

## SEE ALSO

[EVP\\_PKEY\\_CTX\\_new\(3\)](#), [EVP\\_PKEY\\_sign\(3\)](#), [EVP\\_PKEY\\_verify\(3\)](#),  
[EVP\\_PKEY\\_verify\\_recover\(3\)](#),

## HISTORY

This function was added in OpenSSL 1.0.0.

## COPYRIGHT

Copyright 2006–2018 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the OpenSSL license (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>.