

**NAME**

EVP\_PKEY\_get\_default\_digest\_nid, EVP\_PKEY\_get\_default\_digest\_name - get default signature digest

**SYNOPSIS**

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

```
int EVP_PKEY_get_default_digest_name(EVP_PKEY *pkey,  
                                     char *mdname, size_t mdname_sz);  
int EVP_PKEY_get_default_digest_nid(EVP_PKEY *pkey, int *pnid);
```

**DESCRIPTION**

**EVP\_PKEY\_get\_default\_digest\_name()** fills in the default message digest name for the public key signature operations associated with key *pkey* into *mdname*, up to at most *mdname\_sz* bytes including the ending NUL byte. The name could be "UNDEF", signifying that a digest must (for return value 2) or may (for return value 1) be left unspecified.

**EVP\_PKEY\_get\_default\_digest\_nid()** 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. This function is only reliable for legacy keys, which are keys with a **EVP\_PKEY\_ASN1\_METHOD**; these keys have typically been loaded from engines, or created with **EVP\_PKEY\_assign\_RSA(3)** or similar.

**NOTES**

For all current standard OpenSSL public key algorithms SHA256 is returned.

**RETURN VALUES**

**EVP\_PKEY\_get\_default\_digest\_name()** and **EVP\_PKEY\_get\_default\_digest\_nid()** both return 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). They return 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\_digestsign\_supports\_digest(3)**,  
**EVP\_PKEY\_verify(3)**, **EVP\_PKEY\_verify\_recover(3)**,

**HISTORY**

This function was added in OpenSSL 1.0.0.

**COPYRIGHT**

Copyright 2006-2023 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>.