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**.

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 first added to OpenSSL 1.0.0.