Full credit is given to the above companies including the OS that this PDF file was generated!

ed Hat Enterprise Linux Release 9.2 Manual Pages on 'EVP_PKEY_get_default_digest_name.3ossl' comman

$ man EVP_PKEY_get_default_digest_name.3ossl

EVP_PKEY_GET_DEFAULT_DIGEST_NID(3ossOpenEVP_PKEY_GET_DEFAULT_DIGEST_NID(3ossl)

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 no digest should be used.

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 2006-2021 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>.