

EVP_PKEY_verify_recover(3). However, note that these functions do not perform a digest of the data to be signed. Therefore, normally you would use the EVP_DigestSignInit(3) functions for this purpose.

For encryption and decryption see EVP_PKEY_encrypt(3) and EVP_PKEY_decrypt(3) respectively. However, note that these functions perform encryption and decryption only.

As public key encryption is an expensive operation, normally you would wrap an encrypted message in a "digital envelope" using the EVP_SealInit(3) and EVP_OpenInit(3) functions.

The EVP_BytesToKey(3) function provides some limited support for password based encryption. Careful selection of the parameters will provide a PKCS#5 PBKDF1 compatible implementation. However, new applications should not typically use this (preferring, for example, PBKDF2 from PCKS#5).

The EVP_EncodeXXX and EVP_DecodeXXX functions implement base 64 encoding and decoding.

All the symmetric algorithms (ciphers), digests and asymmetric algorithms (public key algorithms) can be replaced by ENGINE modules providing alternative implementations. If ENGINE implementations of ciphers or digests are registered as defaults, then the various EVP functions will automatically use those implementations automatically in preference to built in software implementations. For more information, consult the engine(3) man page.

Although low-level algorithm specific functions exist for many algorithms their use is discouraged. They cannot be used with an ENGINE and ENGINE versions of new algorithms cannot be accessed using the low-level functions. Also makes code harder to adapt to new algorithms and some options are not cleanly supported at the low-level and some operations are more efficient using the high-level interface.

SEE ALSO

EVP_DigestInit(3), EVP_EncryptInit(3), EVP_OpenInit(3), EVP_SealInit(3),
EVP_DigestSignInit(3), EVP_SignInit(3), EVP_VerifyInit(3), EVP_EncodeInit(3),
EVP_PKEY_new(3), EVP_PKEY_fromdata(3), EVP_PKEY_todata(3), EVP_PKEY_keygen(3),
EVP_PKEY_print_private(3), EVP_PKEY_decrypt(3), EVP_PKEY_encrypt(3), EVP_PKEY_sign(3),
EVP_PKEY_verify(3), EVP_PKEY_verify_recover(3), EVP_PKEY_derive(3), EVP_BytesToKey(3),
ENGINE_by_id(3)

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>.

3.0.2

2024-02-16

EVP(7SSL)