NAME

OSSL_PROVIDER-legacy - OpenSSL legacy provider

DESCRIPTION

The OpenSSL legacy provider supplies OpenSSL implementations of algorithms that have been deemed legacy. Such algorithms have commonly fallen out of use, have been deemed insecure by the cryptography community, or something similar.

We can consider this the retirement home of cryptographic algorithms.

Properties

The implementations in this provider specifically has this property defined:

"provider=legacy"

It may be used in a property query string with fetching functions such as **EVP_MD_fetch**(3) or **EVP_CIPHER_fetch**(3), as well as with other functions that take a property query string, such as **EVP_PKEY_CTX_new_from_name**(3).

It isn’t mandatory to query for any of these properties, except to make sure to get implementations of this provider and none other.

OPERATIONS AND ALGORITHMS

The OpenSSL legacy provider supports these operations and algorithms:

Hashing Algorithms / Message Digests

MD2, see **EVP_MD-MD2**(7)
MD4, see **EVP_MD-MD4**(7)
MDC2, see **EVP_MD-MDC2**(7)
WHIRLPOOL, see **EVP_MD-WHIRLPOOL**(7)
RIPEMD160, see **EVP_MD-RIPEMD160**(7)

Symmetric Ciphers

Not all of these symmetric cipher algorithms are enabled by default.

Blowfish, see **EVP_CIPHER-BLOWFISH**(7)
CAST, see **EVP_CIPHER-CAST**(7)
DES, see **EVP_CIPHER-DES**(7)

The algorithm names are: DES_ECB, DES_CBC, DES_OFB, DES_CFB, DES_CFB1, DES_CFB8 and DESX_CBC.

IDEA, see **EVP_CIPHER-IDEA**(7)

RC2, see **EVP_CIPHER-RC2**(7)

RC4, see **EVP_CIPHER-RC4**(7)

RC5, see **EVP_CIPHER-RC5**(7)

Disabled by default. Use *enable-rc5* config option to enable.

SEED, see **EVP_CIPHER-SEED**(7)

Key Derivation Function (KDF)

PBKDF1

SEE ALSO

OSSL_PARAM(3), **openssl-core.h**(7), **openssl-core_dispatch.h**(7), **provider**(7)

HISTORY

This functionality was added in OpenSSL 3.0.

COPYRIGHT