

**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

Copyright 2020-2021 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>.