

**NAME**

EVP\_KEM-RSA – EVP\_KEM RSA keytype and algorithm support

**DESCRIPTION**

The **RSA** keytype and its parameters are described in **EVP\_PKEY-RSA** (7). See **EVP\_PKEY\_encapsulate** (3) and **EVP\_PKEY\_decapsulate** (3) for more info.

**RSA KEM parameters**

“operation” (**OSSL\_KEM\_PARAM\_OPERATION**) <UTF8 string>

The OpenSSL RSA Key Encapsulation Mechanism only currently supports the following operation

“RSASVE”

The encapsulate function simply generates a secret using random bytes and then encrypts the secret using the RSA public key (with no padding). The decapsulate function recovers the secret using the RSA private key.

This can be set using **EVP\_PKEY\_CTX\_set\_kem\_op**().

**CONFORMING TO**

SP800-56Br2

Section 7.2.1.2 RSASVE Generate Operation (RSASVE.GENERATE). Section 7.2.1.3 RSASVE Recovery Operation (RSASVE.RECOVER).

**SEE ALSO**

**EVP\_PKEY\_CTX\_set\_kem\_op** (3), **EVP\_PKEY\_encapsulate** (3), **EVP\_PKEY\_decapsulate** (3)  
**EVP\_KEYMGMT** (3), **EVP\_PKEY** (3), **provider-keymgmt** (7)

**COPYRIGHT**

Copyright 2020 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>>.