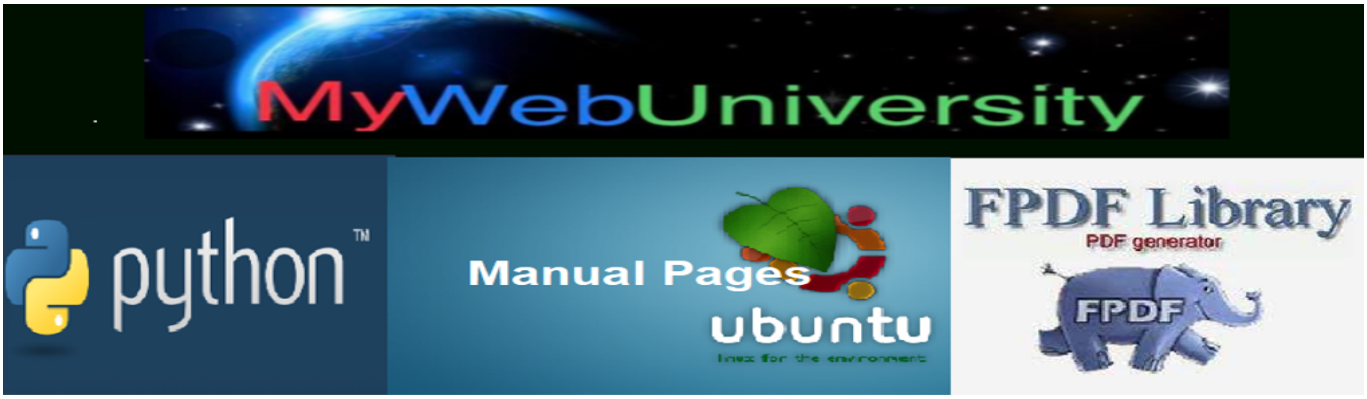

Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP_KEM-RSA.7ssl'

$ man EVP_KEM-RSA.7ssl

EVP_KEM-RSA(7SSL) OpenSSL EVP_KEM-RSA(7SSL)

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