NAME

EVP_ASYM_CIPHER−RSA − RSA Asymmetric Cipher algorithm support

DESCRIPTION

Asymmetric Cipher support for the **RSA** key type.

RSA Asymmetric Cipher parameters

"pad−mode" (**OSSL_ASYM_CIPHER_PARAM_PAD_MODE**) <UTF8 string>

The default provider understands these RSA padding modes in string form:

"none" (**OSSL_PKEY_RSA_PAD_MODE_NONE**)
"oaep" (**OSSL_PKEY_RSA_PAD_MODE_OAEP**)
"pkcs1" (**OSSL_PKEY_RSA_PAD_MODE_PKCSV15**)

This padding mode is no longer supported by the FIPS provider for key agreement and key transport. (This is a FIPS 140−3 requirement). See "OPTIONS" in **openssl−fipsinstall** (1) **−rsa_pkcs15_pad_disabled**.

"x931" (**OSSL_PKEY_RSA_PAD_MODE_X931**)

"pad−mode" (**OSSL_ASYM_CIPHER_PARAM_PAD_MODE**) <integer>

The default provider understands these RSA padding modes in integer form:

1 (**RSA_PKCS1_PADDING**)

This padding mode is no longer supported by the FIPS provider for key agreement and key transport. (This is a FIPS 140−3 requirement)

3 (**RSA_NO_PADDING**)
4 (**RSA_PKCS1_OAEP_PADDING**)
5 (**RSA_X931_PADDING**)

See **EVP_PKEY_CTX_set_rsa_padding** (3) for further details.

"digest" (**OSSL_ASYM_CIPHER_PARAM_OAEP_DIGEST**) <UTF8 string>
"digest−props" (**OSSL_ASYM_CIPHER_PARAM_OAEP_DIGEST_PROPS**) <UTF8 string>
"mgf1−digest" (**OSSL_ASYM_CIPHER_PARAM_MGF1_DIGEST**) <UTF8 string>
"mgf1−digest−props" (**OSSL_ASYM_CIPHER_PARAM_MGF1_DIGEST_PROPS**) <UTF8 string>
"oaep−label" (**OSSL_ASYM_CIPHER_PARAM_OAEP_LABEL**) <octet string>
"tls−client−version" (**OSSL_ASYM_CIPHER_PARAM_TLS_CLIENT_VERSION**) <unsigned integer>

See **RSA_PKCS1_WITH_TLS_PADDING** on the page **EVP_PKEY_CTX_set_rsa_padding** (3).

"tls−negotiated−version" (**OSSL_ASYM_CIPHER_PARAM_TLS_CLIENT_VERSION**) <unsigned integer>

See **RSA_PKCS1_WITH_TLS_PADDING** on the page **EVP_PKEY_CTX_set_rsa_padding** (3).

See "Asymmetric Cipher Parameters" in **provider−asym_cipher** (7) for more information.

The OpenSSL FIPS provider also supports the following parameters:

"fips−indicator" (**OSSL_ASYM_CIPHER_PARAM_FIPS_APPROVED_INDICATOR**) <integer>
"key−check" (**OSSL_ASYM_CIPHER_PARAM_FIPS_KEY_CHECK**) <integer>

See "Asymmetric Cipher Parameters" in **provider−asym_cipher** (7) for more information.

"pkcs15−pad−disabled" (**OSSL_ASYM_CIPHER_PARAM_FIPS_RSA_PKCS15_PAD_DISABLED**) <integer>

The default value of 1 causes an error during encryption if the RSA padding mode is set to "pkcs1". Setting this to zero will ignore the error and set the approved "fips−indicator" to 0. This option breaks FIPS compliance if it causes the approved "fips−indicator" to return 0.

SEE ALSO

EVP_PKEY−RSA (7), **EVP_PKEY** (3), **provider−asym_cipher** (7), **provider−keymgmt** (7), **OSSL_PROVIDER−default** (7) **OSSL_PROVIDER−FIPS** (7)

COPYRIGHT