
***Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP_SIGNATURE-RSA.7ossl'***

***$ man EVP_SIGNATURE-RSA.7ossl***

EVP_SIGNATURE-RSA(7ossl) OpenSSL EVP_SIGNATURE-RSA(7ossl)

NAME

EVP_SIGNATURE-RSA - The EVP_PKEY RSA signature implementation

DESCRIPTION

Support for computing RSA signatures. See EVP_PKEY-RSA(7) for information related to RSA keys.

Signature Parameters

The following signature parameters can be set using EVP_PKEY_CTX_set_params(). This may be called after EVP_PKEY_sign_init() or EVP_PKEY_verify_init(), and before calling EVP_PKEY_sign() or EVP_PKEY_verify().

"digest" (OSSL_SIGNATURE_PARAM_DIGEST) <UTF8 string>

"properties" (OSSL_SIGNATURE_PARAM_PROPERTIES) <UTF8 string>

These common parameters are described in provider-signature(7).

"pad-mode" (OSSL_SIGNATURE_PARAM_PAD_MODE) <UTF8 string>

The type of padding to be used. Its value can be one of the following:

"none" (OSSL_PKEY_RSA_PAD_MODE_NONE)

"pkcs1" (OSSL_PKEY_RSA_PAD_MODE_PKCSV15)

"x931" (OSSL_PKEY_RSA_PAD_MODE_X931)

"pss" (OSSL_PKEY_RSA_PAD_MODE_PSS)

"mgf1-digest" (OSSL_SIGNATURE_PARAM_MGF1_DIGEST) <UTF8 string>

The digest algorithm name to use for the maskGenAlgorithm used by "pss" mode.

"mgf1-properties" (OSSL_SIGNATURE_PARAM_MGF1_PROPERTIES) <UTF8 string>

Sets the name of the property query associated with the "mgf1-digest" algorithm. NULL is used if this optional value is not set.

"saltlen" (OSSL_SIGNATURE_PARAM_PSS_SALTLEN) <integer> or <UTF8 string>

The "pss" mode minimum salt length. The value can either be an integer, a string value representing a number or one of the following string values:

"digest" (OSSL_PKEY_RSA_PSS_SALT_LEN_DIGEST)

Use the same length as the digest size.

"max" (OSSL_PKEY_RSA_PSS_SALT_LEN_MAX)

Use the maximum salt length.

"auto" (OSSL_PKEY_RSA_PSS_SALT_LEN_AUTO)

Auto detect the salt length.

"auto-digestmax" (OSSL_PKEY_RSA_PSS_SALT_LEN_AUTO_DIGEST_MAX)

Auto detect the salt length when verifying. Maximize the salt length up to the digest size when signing to comply with FIPS 186-4 section 5.5.

The following signature parameters can be retrieved using EVP_PKEY_CTX_get_params().

"algorithm-id" (OSSL_SIGNATURE_PARAM_ALGORITHM_ID) <octet string>

This common parameter is described in provider-signature(7).

"digest" (OSSL_SIGNATURE_PARAM_DIGEST) <UTF8 string>

"pad-mode" (OSSL_SIGNATURE_PARAM_PAD_MODE) <UTF8 string>

"mgf1-digest" (OSSL_SIGNATURE_PARAM_MGF1_DIGEST) <UTF8 string>

"saltlen" (OSSL_SIGNATURE_PARAM_PSS_SALTLEN) <integer> or <UTF8 string>

These parameters are as described above.

## SEE ALSO

EVP_PKEY_CTX_set_params(3), EVP_PKEY_sign(3), EVP_PKEY_verify(3), provider-signature(7),

## COPYRIGHT