

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_PKCS15**)

“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.

“pss-saltlen” (**OSSL_SIGNATURE_PARAM_PSS_SALTLEN**) <UTF8 string>

Set or get the “pss” mode minimum salt length. The value can either be a string value representing a number or one of the following:

“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.

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>

These parameters are as described above.

SEE ALSO

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

EVP_PKEY_sign (3),

EVP_PKEY_verify (3),

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>>.