NAME

RSA−PSS − EVP_PKEY RSA−PSS algorithm support

DESCRIPTION

The **RSA-PSS** EVP_PKEY implementation is a restricted version of the RSA algorithm which only supports signing, verification and key generation using PSS padding modes with optional parameter restrictions.

It has associated private key and public key formats.

This algorithm shares several control operations with the **RSA** algorithm but with some restrictions described below.

Signing and Verification

Signing and verification is similar to the **RSA** algorithm except the padding mode is always PSS. If the key in use has parameter restrictions then the corresponding signature parameters are set to the restrictions: for example, if the key can only be used with digest SHA256, MGF1 SHA256 and minimum salt length 32 then the digest, MGF1 digest and salt length will be set to SHA256, SHA256 and 32 respectively.

Key Generation

By default no parameter restrictions are placed on the generated key.

NOTES

The public key format is documented in RFC4055.

The PKCS#8 private key format used for RSA-PSS keys is similar to the RSA format except it uses the **id-RSASSA-PSS** OID and the parameters field, if present, restricts the key parameters in the same way as the public key.

CONFORMING TO

RFC 4055

SEE ALSO

EVP_PKEY_CTX_set_rsa_pss_keygen_md(3), **EVP_PKEY_CTX_set_rsa_pss_keygen_mgf1_md**(3), **EVP_PKEY_CTX_set_rsa_pss_keygen_saltlen**(3), **EVP_PKEY_CTX_new**(3), **EVP_PKEY_CTX_ctrl_str**(3), **EVP_PKEY_derive**(3)

COPYRIGHT