Full credit is given to the above companies including the OS that this PDF file was generated!

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'EVP_PKEY_CTX_settable_params.3ossl' command

$ man EVP_PKEY_CTX_settable_params.3ossl

EVP_PKEY_CTX_SET_PARAMS(3ossl) OpenSSL EVP_PKEY_CTX_SET_PARAMS(3ossl)

NAME

EVP_PKEY_CTX_set_params, EVP_PKEY_CTX_settable_params,

EVP_PKEY_CTX_get_params, EVP_PKEY_CTX_gettable_params - provider

parameter passing operations

SYNOPSIS

```
#include <openssl/evp.h>

int EVP_PKEY_CTX_set_params(EVP_PKEY_CTX *ctx, const OSSL_PARAM *params);

const OSSL_PARAM *EVP_PKEY_CTX_settable_params(const EVP_PKEY_CTX *ctx);

int EVP_PKEY_CTX_get_params(EVP_PKEY_CTX *ctx, OSSL_PARAM *params);

const OSSL_PARAM *EVP_PKEY_CTX_gettable_params(const EVP_PKEY_CTX *ctx);
```

DESCRIPTION

The EVP_PKEY_CTX_get_params() and EVP_PKEY_CTX_set_params() functions allow transfer of arbitrary key parameters to and from providers. Not all parameters may be supported by all providers. See OSSL_PROVIDER(3) for more information on providers. See OSSL_PARAM(3) for more information on parameters. These functions must only be called after the EVP_PKEY_CTX has been initialised for use in an operation. These methods replace the EVP_PKEY_CTX_ctrl() mechanism. (EVP_PKEY_CTX_ctrl now calls these methods internally to interact with providers).

EVP_PKEY_CTX_gettable_params() and EVP_PKEY_CTX_settable_params() get a constant OSSL_PARAM array that describes the gettable and settable parameters for the current algorithm implementation, i.e. parameters

that can be used with EVP_PKEY_CTX_get_params() and EVP_PKEY_CTX_set_params() respectively. See OSSL_PARAM(3) for the use of OSSL_PARAM as parameter descriptor. These functions must only be called after the EVP_PKEY_CTX has been initialised for use in an operation.

Parameters

Examples of EVP_PKEY parameters include the following:

"Common parameters" in provider-keymgmt(7) "Key Exchange parameters" in provider-keyexch(7) "Signature parameters" in provider-signature(7) "Common RSA parameters" in EVP_PKEY-RSA(7) "RSA key generation parameters" in EVP_PKEY-RSA(7) "FFC parameters" in EVP_PKEY-FFC(7) "FFC key generation parameters" in EVP_PKEY-FFC(7) "DSA parameters" in EVP_PKEY-DSA(7) "DSA key generation parameters" in EVP_PKEY-DSA(7) "DH parameters" in EVP_PKEY-DH(7) "DH key generation parameters" in EVP_PKEY-DH(7) "Common EC parameters" in EVP_PKEY-EC(7) "Common X25519, X448, ED25519 and ED448 parameters" in EVP_PKEY-X25519(7)

RETURN VALUES

EVP_PKEY_CTX_set_params() returns 1 for success or 0 otherwise.

EVP_PKEY_CTX_settable_params() returns an OSSL_PARAM array on success or NULL on error. It may also return NULL if there are no settable parameters available.

All other functions and macros described on this page return a positive value for success and 0 or a negative value for failure. In particular a return value of -2 indicates the operation is not supported by the public key algorithm.

SEE ALSO

EVP_PKEY_CTX_new(3), EVP_PKEY_encrypt(3), EVP_PKEY_decrypt(3), EVP_PKEY_sign(3), EVP_PKEY_verify(3), EVP_PKEY_verify_recover(3), EVP_PKEY_derive(3), EVP_PKEY_keygen(3)

HISTORY

All functions were added in OpenSSL 3.0.

COPYRIGHT