

NAME

EVP_CIPHER_CTX_get_algor, EVP_CIPHER_CTX_get_algor_params,
 EVP_CIPHER_CTX_set_algor_params, EVP_PKEY_CTX_get_algor,
 EVP_PKEY_CTX_get_algor_params, EVP_PKEY_CTX_set_algor_params – pass AlgorithmIdentifier
 and its params to/from algorithm implementations

SYNOPSIS

```
int EVP_TYPE_CTX_get_algor(EVP_TYPE_CTX *ctx, X509_ALGOR **alg);
int EVP_TYPE_CTX_get_algor_params(EVP_TYPE_CTX *ctx, X509_ALGOR *alg);
int EVP_TYPE_CTX_set_algor_params(EVP_TYPE_CTX *ctx, const X509_ALGOR *alg);
```

DESCRIPTION

In the description here and the "SYNOPSIS" above, **TYPE** is used as a placeholder for any EVP operation type.

EVP_TYPE_CTX_get_algor() attempts to retrieve a complete AlgorithmIdentifier from the **EVP_TYPE** implementation, and populates **alg* with it. If *alg* is NULL, calling this function will serve to see if calling this function is supported at all by the **EVP_TYPE** implementation. If **alg* is NULL, space will be allocated automatically, and assigned to **alg*.

EVP_TYPE_CTX_get_algor_params() attempts to retrieve the *parameters* part of an AlgorithmIdentifier from the **EVP_TYPE** implementation, and populates *alg->parameters* with it. If *alg* is NULL, calling this function will serve to see if calling this function is supported at all by the **EVP_TYPE** implementation. If *alg->parameters* is NULL, space will be allocated automatically, and assigned to *alg->parameters*. If *alg->parameters* is not NULL, its previous contents will be overwritten with the retrieved AlgorithmIdentifier parameters. Beware!

EVP_TYPE_CTX_set_algor_params() attempts to pass *alg->parameters* to the **EVP_TYPE** implementation. If *alg* is NULL, calling this function will serve to see if calling this function is supported at all by the **EVP_TYPE** implementation.

RETURN VALUES

All functions return 1 for success, and 0 or a negative number if an error occurs. In particular, -2 is returned when the function isn't supported by the **EVP_TYPE** implementation.

HISTORY

These functions were added in OpenSSL 3.4.

COPYRIGHT

Copyright 2024 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>](https://www.openssl.org/source/license.html).