

**NAME**

`EVP_CIPHER_CTX_get_original_iv`, `EVP_CIPHER_CTX_get_updated_iv`, `EVP_CIPHER_CTX_iv`, `EVP_CIPHER_CTX_original_iv`, `EVP_CIPHER_CTX_iv_noconst` - Routines to inspect `EVP_CIPHER_CTX` IV data

**SYNOPSIS**

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

```
int EVP_CIPHER_CTX_get_original_iv(EVP_CIPHER_CTX *ctx, void *buf, size_t len);
int EVP_CIPHER_CTX_get_updated_iv(EVP_CIPHER_CTX *ctx, void *buf, size_t len);
```

The following functions have been deprecated since OpenSSL 3.0, and can be hidden entirely by defining `OPENSSL_API_COMPAT` with a suitable version value, see `openssl_user_macros(7)`:

```
const unsigned char *EVP_CIPHER_CTX_iv(const EVP_CIPHER_CTX *ctx);
const unsigned char *EVP_CIPHER_CTX_original_iv(const EVP_CIPHER_CTX *ctx);
unsigned char *EVP_CIPHER_CTX_iv_noconst(EVP_CIPHER_CTX *ctx);
```

**DESCRIPTION**

`EVP_CIPHER_CTX_get_original_iv()` and `EVP_CIPHER_CTX_get_updated_iv()` copy initialization vector (IV) information from the `EVP_CIPHER_CTX` into the caller-supplied buffer.

`EVP_CIPHER_CTX_get_iv_length(3)` can be used to determine an appropriate buffer size, and if the supplied buffer is too small, an error will be returned (and no data copied).

`EVP_CIPHER_CTX_get_original_iv()` accesses the ("original") IV that was supplied when the `EVP_CIPHER_CTX` was initialized, and `EVP_CIPHER_CTX_get_updated_iv()` accesses the current "IV state" of the cipher, which is updated during cipher operation for certain cipher modes (e.g., CBC and OFB).

The functions `EVP_CIPHER_CTX_iv()`, `EVP_CIPHER_CTX_original_iv()`, and `EVP_CIPHER_CTX_iv_noconst()` are deprecated functions that provide similar (at a conceptual level) functionality. `EVP_CIPHER_CTX_iv()` returns a pointer to the beginning of the "IV state" as maintained internally in the `EVP_CIPHER_CTX`; `EVP_CIPHER_CTX_original_iv()` returns a pointer to the beginning of the ("original") IV, as maintained by the `EVP_CIPHER_CTX`, that was provided when the `EVP_CIPHER_CTX` was initialized; and `EVP_CIPHER_CTX_get_iv_noconst()` is the same as `EVP_CIPHER_CTX_iv()` but has a different return type for the pointer.

**RETURN VALUES**

`EVP_CIPHER_CTX_get_original_iv()` and `EVP_CIPHER_CTX_get_updated_iv()` return 1 on success and 0 on failure.

The functions **EVP\_CIPHER\_CTX\_iv()**, **EVP\_CIPHER\_CTX\_original\_iv()**, and **EVP\_CIPHER\_CTX\_iv\_noconst()** return a pointer to an IV as an array of bytes on success, and NULL on failure.

## HISTORY

**EVP\_CIPHER\_CTX\_get\_original\_iv()** and **EVP\_CIPHER\_CTX\_get\_updated\_iv()** were added in OpenSSL 3.0.0.

**EVP\_CIPHER\_CTX\_iv()**, **EVP\_CIPHER\_CTX\_original\_iv()**, and **EVP\_CIPHER\_CTX\_iv\_noconst()** were added in OpenSSL 1.1.0, and were deprecated in OpenSSL 3.0.0.

## 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>.