



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

***Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP\_aria\_192\_cfb128.3oss1'***

***\$ man EVP\_aria\_192\_cfb128.3oss1***

EVP\_ARIA\_128\_GCM(3oss1)      OpenSSL      EVP\_ARIA\_128\_GCM(3oss1)

**NAME**

EVP\_aria\_128\_cbc, EVP\_aria\_192\_cbc, EVP\_aria\_256\_cbc, EVP\_aria\_128\_cfb,  
EVP\_aria\_192\_cfb, EVP\_aria\_256\_cfb, EVP\_aria\_128\_cfb1,  
EVP\_aria\_192\_cfb1, EVP\_aria\_256\_cfb1, EVP\_aria\_128\_cfb8,  
EVP\_aria\_192\_cfb8, EVP\_aria\_256\_cfb8, EVP\_aria\_128\_cfb128,  
EVP\_aria\_192\_cfb128, EVP\_aria\_256\_cfb128, EVP\_aria\_128\_ctr,  
EVP\_aria\_192\_ctr, EVP\_aria\_256\_ctr, EVP\_aria\_128\_ecb, EVP\_aria\_192\_ecb,  
EVP\_aria\_256\_ecb, EVP\_aria\_128\_ofb, EVP\_aria\_192\_ofb, EVP\_aria\_256\_ofb,  
EVP\_aria\_128\_ccm, EVP\_aria\_192\_ccm, EVP\_aria\_256\_ccm, EVP\_aria\_128\_gcm,  
EVP\_aria\_192\_gcm, EVP\_aria\_256\_gcm, - EVP ARIA cipher

**SYNOPSIS**

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

```
const EVP_CIPHER *EVP_ciphertype(void)
```

EVP\_ciphertype is used as a placeholder for any of the described cipher functions, such as EVP\_aria\_128\_cbc.

## DESCRIPTION

The ARIA encryption algorithm for EVP.

EVP\_aria\_128\_cbc(), EVP\_aria\_192\_cbc(), EVP\_aria\_256\_cbc(),  
EVP\_aria\_128\_cfb(), EVP\_aria\_192\_cfb(), EVP\_aria\_256\_cfb(),  
EVP\_aria\_128\_cfb1(), EVP\_aria\_192\_cfb1(), EVP\_aria\_256\_cfb1(),  
EVP\_aria\_128\_cfb8(), EVP\_aria\_192\_cfb8(), EVP\_aria\_256\_cfb8(),  
EVP\_aria\_128\_cfb128(), EVP\_aria\_192\_cfb128(), EVP\_aria\_256\_cfb128(),  
EVP\_aria\_128\_ctr(), EVP\_aria\_192\_ctr(), EVP\_aria\_256\_ctr(),  
EVP\_aria\_128\_ecb(), EVP\_aria\_192\_ecb(), EVP\_aria\_256\_ecb(),  
EVP\_aria\_128\_ofb(), EVP\_aria\_192\_ofb(), EVP\_aria\_256\_ofb()

ARIA for 128, 192 and 256 bit keys in the following modes: CBC, CFB with 128-bit shift, CFB with 1-bit shift, CFB with 8-bit shift, CTR, ECB and OFB.

EVP\_aria\_128\_ccm(), EVP\_aria\_192\_ccm(), EVP\_aria\_256\_ccm(),  
EVP\_aria\_128\_gcm(), EVP\_aria\_192\_gcm(), EVP\_aria\_256\_gcm(),

ARIA for 128, 192 and 256 bit keys in CBC-MAC Mode (CCM) and Galois Counter Mode (GCM). These ciphers require additional control operations to function correctly, see the "AEAD Interface" in EVP\_EncryptInit(3) section for details.

## RETURN VALUES

These functions return an EVP\_CIPHER structure that contains the implementation of the symmetric cipher. See EVP\_CIPHER\_meth\_new(3) for details of the EVP\_CIPHER structure.

## SEE ALSO

evp(7), EVP\_EncryptInit(3), EVP\_CIPHER\_meth\_new(3)

## COPYRIGHT

Copyright 2017-2019 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>.

3.0.7                    2023-07-13            EVP\_ARIA\_128\_GCM(3ossl)