



*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\_KDF-X942-ASN1.7oss1'***

***\$ man EVP\_KDF-X942-ASN1.7oss1***

EVP\_KDF-X942-ASN1(7oss1)      OpenSSL      EVP\_KDF-X942-ASN1(7oss1)

#### NAME

EVP\_KDF-X942-ASN1 - The X9.42-2003 asn1 EVP\_KDF implementation

#### DESCRIPTION

The EVP\_KDF-X942-ASN1 algorithm implements the key derivation function X942KDF-ASN1. It is used by DH KeyAgreement, to derive a key using input such as a shared secret key and other info. The other info is DER encoded data that contains a 32 bit counter as well as optional fields for "partyu-info", "partyv-info", "supp-pubinfo" and "supp-privinfo".

This kdf is used by Cryptographic Message Syntax (CMS).

#### Identity

"X942KDF-ASN1" or "X942KDF" is the name for this implementation; it can be used with the EVP\_KDF\_fetch() function.

The supported parameters are:

"properties" (OSSL\_KDF\_PARAM\_PROPERTIES) <UTF8 string>

"digest" (OSSL\_KDF\_PARAM\_DIGEST) <UTF8 string>

These parameters work as described in "PARAMETERS" in EVP\_KDF(3).

"secret" (OSSL\_KDF\_PARAM\_SECRET) <octet string>

The shared secret used for key derivation. This parameter sets the secret.

"acvp-info" (OSSL\_KDF\_PARAM\_X942\_ACVPINFO) <octet string>

This value should not be used in production and should only be used for ACVP testing. It is an optional octet string containing a combined DER encoded blob of any of the optional fields related to "partyu-info", "partyv-info", "supp-pubinfo" and "supp-privinfo".

If it is specified then none of these other fields should be used.

"partyu-info" (OSSL\_KDF\_PARAM\_X942\_PARTYUINFO) <octet string>

An optional octet string containing public info contributed by the initiator.

"ukm" (OSSL\_KDF\_PARAM\_UKM) <octet string>

An alias for "partyu-info". In CMS this is the user keying material.

"partyv-info" (OSSL\_KDF\_PARAM\_X942\_PARTYVINFO) <octet string>

An optional octet string containing public info contributed by the responder.

"supp-pubinfo" (OSSL\_KDF\_PARAM\_X942\_SUPP\_PUBINFO) <octet string>

An optional octet string containing some additional, mutually-known public information. Setting this value also sets "use-keybits" to

0.

"use-keybits" (OSSL\_KDF\_PARAM\_X942\_USE\_KEYBITS) <integer>

The default value of 1 will use the KEK key length (in bits) as the "supp-pubinfo". A value of 0 disables setting the "supp-pubinfo".

"supp-privinfo" (OSSL\_KDF\_PARAM\_X942\_SUPP\_PRIVINFO) <octet string>

An optional octet string containing some additional, mutually-known private information.

"cekalg" (OSSL\_KDF\_PARAM\_CEK\_ALG) <UTF8 string>

This parameter sets the CEK wrapping algorithm name. Valid values are "AES-128-WRAP", "AES-192-WRAP", "AES-256-WRAP" and "DES3-WRAP".

## NOTES

A context for X942KDF can be obtained by calling:

```
EVP_KDF *kdf = EVP_KDF_fetch(NULL, "X942KDF", NULL);  
EVP_KDF_CTX *kctx = EVP_KDF_CTX_new(kdf);
```

The output length of an X942KDF is specified via the keylen parameter to the EVP\_KDF\_derive(3) function.

## EXAMPLES

This example derives 24 bytes, with the secret key "secret" and random user keying material:

```
EVP_KDF_CTX *kctx;  
EVP_KDF_CTX *kctx;  
unsigned char out[192/8];  
unsigned char ukm[64];  
OSSL_PARAM params[5], *p = params;  
  
if (RAND_bytes(ukm, sizeof(ukm)) <= 0)
```

```

error("RAND_bytes");

kdf = EVP_KDF_fetch(NULL, "X942KDF", NULL);
if (kctx == NULL)
    error("EVP_KDF_fetch");
kctx = EVP_KDF_CTX_new(kdf);
EVP_KDF_free(kdf);
if (kctx == NULL)
    error("EVP_KDF_CTX_new");

*p++ = OSSL_PARAM_construct_utf8_string(OSSL_KDF_PARAM_DIGEST, "SHA256", 0);
*p++ = OSSL_PARAM_construct_octet_string(OSSL_KDF_PARAM_SECRET,
                                         "secret", (size_t)6);
*p++ = OSSL_PARAM_construct_octet_string(OSSL_KDF_PARAM_UKM, ukm, sizeof(ukm));
*p++ = OSSL_PARAM_construct_utf8_string(OSSL_KDF_PARAM_CEK_ALG, "AES-256-WRAP", 0);
*p = OSSL_PARAM_construct_end();
if (EVP_KDF_derive(kctx, out, sizeof(out), params) <= 0)
    error("EVP_KDF_derive");

EVP_KDF_CTX_free(kctx);

```

## CONFORMING TO

ANS1 X9.42-2003 RFC 2631

## SEE ALSO

EVP\_KDF(3), EVP\_KDF\_CTX\_new(3), EVP\_KDF\_CTX\_free(3),  
EVP\_KDF\_CTX\_set\_params(3), EVP\_KDF\_CTX\_get\_kdf\_size(3),  
EVP\_KDF\_derive(3), "PARAMETERS" in EVP\_KDF(3)

## HISTORY

This functionality was added to OpenSSL 3.0.

Copyright 2019-2022 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\_KDF-X942-ASN1(7ossl)