## 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.

### Supported parameters

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).

‘‘key’’ (**OSSL_KDF_PARAM_KEY**) <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_SUPP_PRIVINFO**) <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];
unsignred 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,
*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