

NAME

EVP_KDF-X942-CONCAT – The X942 Concat EVP_KDF implementation

DESCRIPTION

The EVP_KDF-X942-CONCAT algorithm is identical to EVP_KDF-X963. It is used for key agreement to derive a key using input such as a shared secret key and shared info.

Identity

“X942KDF_CONCAT” is the name for this implementation; it can be used with the **EVP_KDF_fetch()** function.

This is an alias for “X963KDF”.

See **EVP_KDF-X963** (7) for a list of supported parameters and examples.

HISTORY

This functionality was added to OpenSSL 3.0.

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