

NAME

EVP_KEYEXCH-X25519, EVP_KEYEXCH-X448 – X25519 and X448 Key Exchange algorithm support

DESCRIPTION

Key exchange support for the **X25519** and **X448** key types.

Key exchange parameters

“pad” (**OSSL_EXCHANGE_PARAM_PAD**) <unsigned integer>

See “Common Key Exchange parameters” in **provider-keyexch** (7).

EXAMPLES

Keys for the host and peer can be generated as shown in “Examples” in **EVP_PKEY-X25519** (7).

The code to generate a shared secret is identical to “Examples” in **EVP_KEYEXCH-DH** (7).

SEE ALSO

EVP_PKEY-FFC (7), **EVP_PKEY-DH** (7) **EVP_PKEY** (3), **provider-keyexch** (7), **provider-keymgmt** (7), **OSSL_PROVIDER-default** (7), **OSSL_PROVIDER-FIPS** (7),

COPYRIGHT

Copyright 2020 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>>.