Happy Key: HPKE implementation (RFC9180)

https://github.com/sftcd/happykey

Generated by Doxygen 1.9.1

Chapter 1

Data Structure Index

1.1 Data Structures

Here are the data structures with brief descriptions:

Chapter 2

Data Structure Documentation

2.1 ossl_hpke_ctx_st Struct Reference

sender or receiver context

Data Fields

- OSSL_LIB_CTX * libctx
  library context
- char * propq
  properties
- int mode
  HPKE mode.
- OSSL_HPKE_SUITE suite
  suite
- uint64_t seq
  aead sequence number
- unsigned char * **shared_secret**
- size_t **shared_secretlen**
- unsigned char * **key**
- size_t **keylen**
- unsigned char * **nonce**
- size_t **noncelen**
- unsigned char * exportersec
  exporter secret
- size_t **exporterseclen**
- char * pskid
  PSK stuff.
- unsigned char * **psk**
- size_t **psklen**
- EVP_PKEY * authpriv
  sender's authentication private key
- unsigned char * authpub
  auth public key
- size_t **authpublen**
- unsigned char * **ikme**
- size_t **ikmelen**

2.1.1 Detailed Description

sender or receiver context

The documentation for this struct was generated from the following file:

- hpke.c

Index