

Navigate...

- [Home](#)
- [Blog](#)
- [Downloads](#)
- [Docs](#)
- [News](#)
- [Policies](#)
- [Community](#)
- [Support](#)

OpenSSL libraries

This is the OpenSSL API for the SSL and Crypto libraries. The [ssl](#) and [crypto](#) manpages are general overviews of those libraries.

NAME	Description
ASN1_add_oid_module	add standard configuration modules
ASN1_generate_nconf	ASN1 generation functions
ASN1_generate_v3	ASN1 generation functions
ASN1_OBJECT_free	object allocation functions
ASN1_OBJECT_new	object allocation functions
ASN1_STRING_cmp	ASN1_STRING utility functions
ASN1_STRING_data	ASN1_STRING utility functions
ASN1_STRING_dup	ASN1_STRING utility functions
ASN1_STRING_free	ASN1_STRING allocation functions
ASN1_STRING_length	ASN1_STRING utility functions
ASN1_STRING_length_set	ASN1_STRING utility functions
ASN1_STRING_new	ASN1_STRING allocation functions
ASN1_STRING_print_ex_fp	ASN1_STRING output routines.
ASN1_STRING_print_ex	ASN1_STRING output routines.
ASN1_STRING_print	ASN1_STRING output routines.
ASN1_STRING_set	ASN1_STRING utility functions
ASN1_STRING_to_UTF8	ASN1_STRING utility functions
ASN1_STRING_type	ASN1_STRING utility functions
ASN1_STRING_type_new	ASN1_STRING allocation functions
ASN1_TIME_adj	ASN.1 Time functions.
ASN1_TIME_check	ASN.1 Time functions.
ASN1_TIME_diff	ASN.1 Time functions.
ASN1_TIME_print	ASN.1 Time functions.

<u>ASN1_TIME_set</u>	ASN.1 Time functions.
<u>ASN1_TIME_set_string</u>	ASN.1 Time functions.
<u>BF_cbc_encrypt</u>	Blowfish encryption
<u>BF_cfb64_encrypt</u>	Blowfish encryption
<u>BF_decrypt</u>	Blowfish encryption
<u>BF_ecb_encrypt</u>	Blowfish encryption
<u>BF_encrypt</u>	Blowfish encryption
<u>BF_ofb64_encrypt</u>	Blowfish encryption
<u>BF_options</u>	Blowfish encryption
<u>BF_set_key</u>	Blowfish encryption
<u>BIO_append_filename</u>	FILE bio
<u>BIO_callback_ctrl</u>	BIO control operations
<u>BIO_ctrl_get_read_request</u>	BIO pair BIO
<u>BIO_ctrl_get_write_guarantee</u>	BIO pair BIO
<u>BIO_ctrl</u>	BIO control operations
<u>BIO_ctrl_pending</u>	BIO control operations
<u>BIO_ctrl_reset_read_request</u>	BIO pair BIO
<u>BIO_ctrl_wpending</u>	BIO control operations
<u>BIO_debug_callback</u>	BIO callback functions
<u>BIO_destroy_bio_pair</u>	BIO pair BIO
<u>BIO_do_accept</u>	accept BIO
<u>BIO_do_connect</u>	connect BIO
<u>BIO_eof</u>	BIO control operations
<u>BIO_f_base64</u>	base64 BIO filter
<u>BIO_f_buffer</u>	buffering BIO
<u>BIO_f_cipher</u>	cipher BIO filter
<u>BIO_find_type</u>	BIO chain traversal
<u>BIO_flush</u>	BIO control operations
<u>BIO_f_md</u>	message digest BIO filter
<u>BIO_f_null</u>	null filter
<u>BIO_free_all</u>	BIO allocation and freeing functions
<u>BIO_free</u>	BIO allocation and freeing functions
<u>BIO_f_ssl</u>	SSL BIO
<u>BIO_get_accept_port</u>	accept BIO
<u>BIO_get_bind_mode</u>	accept BIO
<u>BIO_get_callback_arg</u>	BIO callback functions
<u>BIO_get_callback</u>	BIO callback functions
<u>BIO_get_cipher_ctx</u>	cipher BIO filter
<u>BIO_get_cipher_status</u>	cipher BIO filter
<u>BIO_get_close</u>	BIO control operations
<u>BIO_get_conn_hostname</u>	connect BIO
<u>BIO_get_conn_int_port</u>	connect BIO
<u>BIO_get_conn_ip</u>	connect BIO
<u>BIO_get_conn_port</u>	connect BIO
<u>BIO_get_fd</u>	file descriptor BIO
<u>BIO_get_fp</u>	FILE bio
<u>BIO_get_info_callback</u>	BIO control operations
<u>BIO_get_md_ctx</u>	message digest BIO filter
<u>BIO_get_md</u>	message digest BIO filter

<u>BIO_get_mem_data</u>	memory BIO
<u>BIO_get_mem_ptr</u>	memory BIO
<u>BIO_get_num_renegotiates</u>	SSL BIO
<u>BIO_get_read_request</u>	BIO pair BIO
<u>BIO_get_retry_BIO</u>	BIO retry functions
<u>BIO_get_retry_reason</u>	BIO retry functions
<u>BIO_gets</u>	BIO I/O functions
<u>BIO_get_ssl</u>	SSL BIO
<u>BIO_get_write_buf_size</u>	BIO pair BIO
<u>BIO_get_write_guarantee</u>	BIO pair BIO
<u>bio</u>	I/O abstraction
<u>BIO_int_ctrl</u>	BIO control operations
<u>BIO_make_bio_pair</u>	BIO pair BIO
<u>BIO_method_type</u>	BIO chain traversal
<u>BIO_new_accept</u>	accept BIO
<u>BIO_new_bio_pair</u>	BIO pair BIO
<u>BIO_new_buffer_ssl_connect</u>	SSL BIO
<u>BIO_new_CMS</u>	CMS streaming filter BIO
<u>BIO_new_connect</u>	connect BIO
<u>BIO_new_fd</u>	file descriptor BIO
<u>BIO_new_file</u>	FILE bio
<u>BIO_new_fp</u>	FILE bio
<u>BIO_new</u>	BIO allocation and freeing functions
<u>BIO_new_mem_buf</u>	memory BIO
<u>BIO_new_socket</u>	socket BIO
<u>BIO_new_ssl_connect</u>	SSL BIO
<u>BIO_new_ssl</u>	SSL BIO
<u>BIO_next</u>	BIO chain traversal
<u>BIO_pending</u>	BIO control operations
<u>BIO_pop</u>	add and remove BIOs from a chain.
<u>BIO_ptr_ctrl</u>	BIO control operations
<u>BIO_push</u>	add and remove BIOs from a chain.
<u>BIO_puts</u>	BIO I/O functions
<u>BIO_read_filename</u>	FILE bio
<u>BIO_read</u>	BIO I/O functions
<u>BIO_reset</u>	BIO control operations
<u>BIO_retry_type</u>	BIO retry functions
<u>BIO_rw_filename</u>	FILE bio
<u>BIO_s_accept</u>	accept BIO
<u>BIO_s_bio</u>	BIO pair BIO
<u>BIO_s_connect</u>	connect BIO
<u>BIO_seek</u>	BIO control operations
<u>BIO_set_accept_bios</u>	accept BIO
<u>BIO_set_accept_port</u>	accept BIO
<u>BIO_set_bind_mode</u>	accept BIO
<u>BIO_set_callback_arg</u>	BIO callback functions
<u>BIO_set_callback</u>	BIO callback functions
<u>BIO_set_cipher</u>	cipher BIO filter
<u>BIO_set_close</u>	BIO control operations

<u>BIO_set_conn_hostname</u>	connect BIO
<u>BIO_set_conn_int_port</u>	connect BIO
<u>BIO_set_conn_ip</u>	connect BIO
<u>BIO_set_conn_port</u>	connect BIO
<u>BIO_set_fd</u>	file descriptor BIO
<u>BIO_set_fp</u>	FILE bio
<u>BIO_set</u>	BIO allocation and freeing functions
<u>BIO_set_info_callback</u>	BIO control operations
<u>BIO_set_md</u>	message digest BIO filter
<u>BIO_set_mem_buf</u>	memory BIO
<u>BIO_set_mem_eof_return</u>	memory BIO
<u>BIO_set_nbio_accept</u>	accept BIO
<u>BIO_set_nbio</u>	connect BIO
<u>BIO_set_ssl</u>	SSL BIO
<u>BIO_set_ssl_mode</u>	SSL BIO
<u>BIO_set_ssl_renegotiate_bytes</u>	SSL BIO
<u>BIO_set_ssl_renegotiate_timeout</u>	SSL BIO
<u>BIO_set_write_buf_size</u>	BIO pair BIO
<u>BIO_s_fd</u>	file descriptor BIO
<u>BIO_s_file</u>	FILE bio
<u>BIO_should_io_special</u>	BIO retry functions
<u>BIO_should_read</u>	BIO retry functions
<u>BIO_should_retry</u>	BIO retry functions
<u>BIO_should_write</u>	BIO retry functions
<u>BIO_shutdown_wr</u>	BIO pair BIO
<u>BIO_s_mem</u>	memory BIO
<u>BIO_s_null</u>	null data sink
<u>BIO_ssl_copy_session_id</u>	SSL BIO
<u>BIO_ssl_shutdown</u>	SSL BIO
<u>BIO_s_socket</u>	socket BIO
<u>BIO_tell</u>	BIO control operations
<u>BIO_vfree</u>	BIO allocation and freeing functions
<u>BIO_wpending</u>	BIO control operations
<u>BIO_write_filename</u>	FILE bio
<u>BIO_write</u>	BIO I/O functions
<u>blowfish</u>	Blowfish encryption
<u>BN_add</u>	arithmetic operations on BIGNUMs
<u>BN_add_word</u>	arithmetic functions on BIGNUMs with integers
<u>bn_add_words</u>	BIGNUM library internal functions
<u>BN_bin2bn</u>	format conversions
<u>BN_BLINDING_convert_ex</u>	blinding related BIGNUM functions.
<u>BN_BLINDING_convert</u>	blinding related BIGNUM functions.
<u>BN_BLINDING_create_param</u>	blinding related BIGNUM functions.
<u>BN_BLINDING_free</u>	blinding related BIGNUM functions.
<u>BN_BLINDING_get_flags</u>	blinding related BIGNUM functions.
<u>BN_BLINDING_get_thread_id</u>	blinding related BIGNUM functions.
<u>BN_BLINDING_invert_ex</u>	blinding related BIGNUM functions.
<u>BN_BLINDING_invert</u>	blinding related BIGNUM functions.
<u>BN_BLINDING_new</u>	blinding related BIGNUM functions.

<u>BN_BLINDING_set_flags</u>	blinding related BIGNUM functions.
<u>BN_BLINDING_set_thread_id</u>	blinding related BIGNUM functions.
<u>BN_BLINDING_thread_id</u>	blinding related BIGNUM functions.
<u>BN_BLINDING_update</u>	blinding related BIGNUM functions.
<u>BN_bn2bin</u>	format conversions
<u>BN_bn2dec</u>	format conversions
<u>BN_bn2hex</u>	format conversions
<u>BN_bn2mpi</u>	format conversions
<u>bn_check_top</u>	BIGNUM library internal functions
<u>BN_clear_bit</u>	bit operations on BIGNUMs
<u>BN_clear_free</u>	allocate and free BIGNUMs
<u>BN_clear</u>	allocate and free BIGNUMs
<u>BN_cmp</u>	BIGNUM comparison and test functions
<u>bn_cmp_words</u>	BIGNUM library internal functions
<u>BN_copy</u>	copy BIGNUMs
<u>BN_CTX_end</u>	use temporary BIGNUM variables
<u>BN_CTX_free</u>	allocate and free BN_CTX structures
<u>BN_CTX_get</u>	use temporary BIGNUM variables
<u>BN_CTX_init</u>	allocate and free BN_CTX structures
<u>BN_CTX_new</u>	allocate and free BN_CTX structures
<u>BN_CTX_start</u>	use temporary BIGNUM variables
<u>BN_dec2bn</u>	format conversions
<u>BN_div</u>	arithmetic operations on BIGNUMs
<u>BN_div_recp</u>	modular multiplication using reciprocal
<u>BN_div_word</u>	arithmetic functions on BIGNUMs with integers
<u>bn_div_words</u>	BIGNUM library internal functions
<u>bn_dump</u>	BIGNUM library internal functions
<u>BN_dup</u>	copy BIGNUMs
<u>bn_expand2</u>	BIGNUM library internal functions
<u>bn_expand</u>	BIGNUM library internal functions
<u>BN_exp</u>	arithmetic operations on BIGNUMs
<u>bn_fix_top</u>	BIGNUM library internal functions
<u>BN_free</u>	allocate and free BIGNUMs
<u>BN_from_montgomery</u>	Montgomery multiplication
<u>BN_gcd</u>	arithmetic operations on BIGNUMs
<u>BN_GENCB_call</u>	generate primes and test for primality
<u>BN_GENCB_set</u>	generate primes and test for primality
<u>BN_GENCB_set_old</u>	generate primes and test for primality
<u>BN_generate_prime_ex</u>	generate primes and test for primality
<u>BN_generate_prime</u>	generate primes and test for primality
<u>BN_get_word</u>	BIGNUM assignment operations
<u>BN_hex2bn</u>	format conversions
<u>bn</u>	multiprecision integer arithmetics
<u>BN_init</u>	allocate and free BIGNUMs
<u>bn_internal</u>	BIGNUM library internal functions
<u>BN_is_bit_set</u>	bit operations on BIGNUMs
<u>BN_is_odd</u>	BIGNUM comparison and test functions
<u>BN_is_one</u>	BIGNUM comparison and test functions
<u>BN_is_prime_ex</u>	generate primes and test for primality

<u>BN_is_prime_fasttest_ex</u>	generate primes and test for primality
<u>BN_is_prime_fasttest</u>	generate primes and test for primality
<u>BN_is_prime</u>	generate primes and test for primality
<u>BN_is_word</u>	BIGNUM comparison and test functions
<u>BN_is_zero</u>	BIGNUM comparison and test functions
<u>BN_lshift1</u>	bit operations on BIGNUMs
<u>BN_lshift</u>	bit operations on BIGNUMs
<u>BN_mask_bits</u>	bit operations on BIGNUMs
<u>BN_mod_add</u>	arithmetic operations on BIGNUMs
<u>BN_mod_exp</u>	arithmetic operations on BIGNUMs
<u>BN_mod</u>	arithmetic operations on BIGNUMs
<u>BN_mod_inverse</u>	compute inverse modulo n
<u>BN_mod_mul</u>	arithmetic operations on BIGNUMs
<u>BN_mod_mul_montgomery</u>	Montgomery multiplication
<u>BN_mod_mul_reciprocal</u>	modular multiplication using reciprocal
<u>BN_mod_sqr</u>	arithmetic operations on BIGNUMs
<u>BN_mod_sub</u>	arithmetic operations on BIGNUMs
<u>BN_mod_word</u>	arithmetic functions on BIGNUMs with integers
<u>BN_MONT_CTX_copy</u>	Montgomery multiplication
<u>BN_MONT_CTX_free</u>	Montgomery multiplication
<u>BN_MONT_CTX_init</u>	Montgomery multiplication
<u>BN_MONT_CTX_new</u>	Montgomery multiplication
<u>BN_MONT_CTX_set</u>	Montgomery multiplication
<u>BN_mpi2bn</u>	format conversions
<u>bn_mul_add_words</u>	BIGNUM library internal functions
<u>bn_mul_comba4</u>	BIGNUM library internal functions
<u>bn_mul_comba8</u>	BIGNUM library internal functions
<u>bn_mul_high</u>	BIGNUM library internal functions
<u>BN_mul</u>	arithmetic operations on BIGNUMs
<u>bn_mul_low_normal</u>	BIGNUM library internal functions
<u>bn_mul_low_recursive</u>	BIGNUM library internal functions
<u>bn_mul_normal</u>	BIGNUM library internal functions
<u>bn_mul_part_recursive</u>	BIGNUM library internal functions
<u>bn_mul_recursive</u>	BIGNUM library internal functions
<u>BN_mul_word</u>	arithmetic functions on BIGNUMs with integers
<u>bn_mul_words</u>	BIGNUM library internal functions
<u>BN_new</u>	allocate and free BIGNUMs
<u>BN_nnmod</u>	arithmetic operations on BIGNUMs
<u>BN_num_bits</u>	get BIGNUM size
<u>BN_num_bits_word</u>	get BIGNUM size
<u>BN_num_bytes</u>	get BIGNUM size
<u>BN_one</u>	BIGNUM assignment operations
<u>BN_print_fp</u>	format conversions
<u>bn_print</u>	BIGNUM library internal functions
<u>BN_print</u>	format conversions
<u>BN_pseudo_rand</u>	generate pseudo-random number
<u>BN_pseudo_rand_range</u>	generate pseudo-random number
<u>BN_rand</u>	generate pseudo-random number
<u>BN_rand_range</u>	generate pseudo-random number

<u>BN_RECP_CTX_free</u>	modular multiplication using reciprocal
<u>BN_RECP_CTX_init</u>	modular multiplication using reciprocal
<u>BN_RECP_CTX_new</u>	modular multiplication using reciprocal
<u>BN_RECP_CTX_set</u>	modular multiplication using reciprocal
<u>BN_rshift1</u>	bit operations on BIGNUMs
<u>BN_rshift</u>	bit operations on BIGNUMs
<u>BN_set_bit</u>	bit operations on BIGNUMs
<u>bn_set_high</u>	BIGNUM library internal functions
<u>bn_set_low</u>	BIGNUM library internal functions
<u>bn_set_max</u>	BIGNUM library internal functions
<u>BN_set_word</u>	BIGNUM assignment operations
<u>bn_sqr_comba4</u>	BIGNUM library internal functions
<u>bn_sqr_comba8</u>	BIGNUM library internal functions
<u>BN_sqr</u>	arithmetic operations on BIGNUMs
<u>bn_sqr_normal</u>	BIGNUM library internal functions
<u>bn_sqr_recursive</u>	BIGNUM library internal functions
<u>bn_sqr_words</u>	BIGNUM library internal functions
<u>BN_sub</u>	arithmetic operations on BIGNUMs
<u>BN_sub_word</u>	arithmetic functions on BIGNUMs with integers
<u>bn_sub_words</u>	BIGNUM library internal functions
<u>BN_swap</u>	exchange BIGNUMs
<u>BN_to_montgomery</u>	Montgomery multiplication
<u>BN_ucmp</u>	BIGNUM comparison and test functions
<u>BN_value_one</u>	BIGNUM assignment operations
<u>bn_wexpand</u>	BIGNUM library internal functions
<u>BN_zero</u>	BIGNUM assignment operations
<u>buffer</u>	standard C library equivalents
<u>BUF_memdup</u>	standard C library equivalents
<u>BUF_MEM_free</u>	standard C library equivalents
<u>BUF_MEM_grow</u>	standard C library equivalents
<u>BUF_MEM_new_ex</u>	standard C library equivalents
<u>BUF_MEM_new</u>	standard C library equivalents
<u>BUF_strdup</u>	standard C library equivalents
<u>BUF_strlcat</u>	standard C library equivalents
<u>BUF_strlepy</u>	standard C library equivalents
<u>BUF_strndup</u>	standard C library equivalents
<u>CMS_add0_cert</u>	CMS certificate and CRL utility functions
<u>CMS_add0_crl</u>	CMS certificate and CRL utility functions
<u>CMS_add0_recipient_key</u>	add recipients to a CMS enveloped data structure
<u>CMS_add1_cert</u>	CMS certificate and CRL utility functions
<u>CMS_add1_crl</u>	CMS certificate and CRL utility functions
<u>CMS_add1_ReceiptRequest</u>	CMS signed receipt request functions.
<u>CMS_add1_recipient_cert</u>	add recipients to a CMS enveloped data structure
<u>CMS_add1_signer</u>	add a signer to a CMS_ContentInfo signed data structure.
<u>CMS_compress</u>	create a CMS CompressedData structure
<u>CMS_decrypt</u>	decrypt content from a CMS envelopedData structure
<u>CMS_encrypt</u>	create a CMS envelopedData structure
<u>CMS_final</u>	finalise a CMS_ContentInfo structure

CMS_get0_content	get and set CMS content types and content
CMS_get0_eContentType	get and set CMS content types and content
CMS_get0_RecipientInfos	CMS envelopedData RecipientInfo routines
CMS_get0_SignerInfos	CMS signedData signer functions.
CMS_get0_signers	verify a CMS SignedData structure
CMS_get0_type	get and set CMS content types and content
CMS_get1_certs	CMS certificate and CRL utility functions
CMS_get1_crls	CMS certificate and CRL utility functions
CMS_get1_ReceiptRequest	CMS signed receipt request functions.
CMS_ReceiptRequest_create0	CMS signed receipt request functions.
CMS_ReceiptRequest_get0_values	CMS signed receipt request functions.
CMS_RecipientInfo_decrypt	CMS envelopedData RecipientInfo routines
CMS_RecipientInfo_encrypt	CMS envelopedData RecipientInfo routines
CMS_RecipientInfo_kekri_get0_id	CMS envelopedData RecipientInfo routines
CMS_RecipientInfo_kekri_id_cmp	CMS envelopedData RecipientInfo routines
CMS_RecipientInfo_ktri_cert_cmp	CMS envelopedData RecipientInfo routines
CMS_RecipientInfo_ktri_get0_signer_id	CMS envelopedData RecipientInfo routines
CMS_RecipientInfo_set0_key	CMS envelopedData RecipientInfo routines
CMS_RecipientInfo_set0_pkey	CMS envelopedData RecipientInfo routines
CMS_RecipientInfo_type	CMS envelopedData RecipientInfo routines
CMS_set1_eContentType	get and set CMS content types and content
CMS_set1_signer_cert	CMS signedData signer functions.
CMS_SignerInfo_cert_cmp	CMS signedData signer functions.
CMS_SignerInfo_get0_signature	CMS signedData signer functions.
CMS_SignerInfo_get0_signer_id	CMS signedData signer functions.
CMS_SignerInfo_sign	add a signer to a CMS_ContentInfo signed data structure.
CMS_sign	create a CMS SignedData structure
CMS_sign_receipt	create a CMS signed receipt
CMS_uncompress	uncompress a CMS CompressedData structure
CMS_verify	verify a CMS SignedData structure
CMS_verify_receipt	verify a CMS signed receipt
CONF_modules_finish	OpenSSL configuration cleanup functions
CONF_modules_free	OpenSSL configuration cleanup functions
CONF_modules_load_file	OpenSSL configuration functions
CONF_modules_load	OpenSSL configuration functions
CONF_modules_unload	OpenSSL configuration cleanup functions
CRYPTO_destroy_dynlockid	OpenSSL thread support
CRYPTO_get_ex_data	internal application specific data functions
CRYPTO_get_new_dynlockid	OpenSSL thread support
crypto	OpenSSL cryptographic library
CRYPTO_lock	OpenSSL thread support
CRYPTO_num_locks	OpenSSL thread support
CRYPTO_set_dynlock_create_callback	OpenSSL thread support
CRYPTO_set_dynlock_destroy_callback	OpenSSL thread support
CRYPTO_set_dynlock_lock_callback	OpenSSL thread support
CRYPTO_set_ex_data	internal application specific data functions
CRYPTO_set_locking_callback	OpenSSL thread support
CRYPTO_THREADID_cmp	OpenSSL thread support

[CRYPTO_THREADID_cpy](#)
[CRYPTO_THREADID_current](#)
[CRYPTO_THREADID_get_callback](#)
[CRYPTO_THREADID_hash](#)
[CRYPTO_THREADID_set_callback](#)
[d2i_ASN1_OBJECT](#)

[d2i_AutoPrivateKey](#)

[d2i_CMS_ContentInfo](#)

[d2i_DHparams](#)

[d2i_DSAParams](#)

[d2i_DSAPrivateKey](#)

[d2i_DSA_PUBKEY](#)

[d2i_DSAPublicKey](#)

[d2i_DSA_SIG](#)

[d2i_ECDSA_SIG](#)

[d2i_ECPKParameters_bio](#)

[d2i_ECPKParameters_fp](#)

[d2i_ECPKParameters](#)

[d2i_ECPrivate_key](#)

[d2i_ECPrivateKey](#)

[d2i_Netscape_RSA](#)

[d2i_PKCS8PrivateKey_bio](#)

[d2i_PKCS8PrivateKey_fp](#)

[d2i_PKCS8PrivateKey](#)

[d2i_Private_key](#)

[d2i_PrivateKey](#)

[d2i_RSAPrivateKey](#)

[d2i_RSA_PUBKEY](#)

[d2i_RSAPublicKey](#)

[d2i_SSL_SESSION](#)

[d2i_X509_ALGOR](#)

[d2i_X509_bio](#)

[d2i_X509_CRL_bio](#)

[d2i_X509_CRL_fp](#)

[d2i_X509_CRL](#)

[d2i_X509_fp](#)

[d2i_X509](#)

[d2i_X509_NAME](#)

[d2i_X509_REQ_bio](#)

[d2i_X509_REQ_fp](#)

OpenSSL thread support

OpenSSL thread support

OpenSSL thread support

OpenSSL thread support

OpenSSL thread support

ASN1 OBJECT IDENTIFIER functions

decode and encode functions for reading and saving
EVP_PKEY structures.

CMS ContentInfo functions

PKCS#3 DH parameter functions.

DSA key encoding and parsing functions.

DSA key encoding and parsing functions.

DSA key encoding and parsing functions.

DSA key encoding and parsing functions.

DSA key encoding and parsing functions.

Elliptic Curve Digital Signature Algorithm

Functions for decoding and encoding ASN1
representations of elliptic curve entities

Functions for decoding and encoding ASN1
representations of elliptic curve entities

Functions for decoding and encoding ASN1
representations of elliptic curve entities

Encode and decode functions for saving and reading
EC_KEY structures

Encode and decode functions for saving and reading
EC_KEY structures

RSA public and private key encoding functions.

PKCS#8 format private key functions

PKCS#8 format private key functions

PKCS#8 format private key functions

decode and encode functions for reading and saving
EVP_PKEY structures.

decode and encode functions for reading and saving
EVP_PKEY structures.

RSA public and private key encoding functions.

RSA public and private key encoding functions.

RSA public and private key encoding functions.

convert SSL_SESSION object from/to ASN1
representation

AlgorithmIdentifier functions.

X509 encode and decode functions

PKCS#10 certificate request functions.

PKCS#10 certificate request functions.

PKCS#10 certificate request functions.

X509 encode and decode functions

X509 encode and decode functions

X509_NAME encoding functions

PKCS#10 certificate request functions.

PKCS#10 certificate request functions.

<u>d2i_X509_REQ</u>	PKCS#10 certificate request functions.
<u>d2i_X509_SIG</u>	DigestInfo functions.
<u>DES_cbc_cksum</u>	DES encryption
<u>DES_cfb64_encrypt</u>	DES encryption
<u>DES_cfb_encrypt</u>	DES encryption
<u>DES_crypt</u>	DES encryption
<u>DES_ecb2_encrypt</u>	DES encryption
<u>DES_ecb3_encrypt</u>	DES encryption
<u>DES_ecb_encrypt</u>	DES encryption
<u>DES_edc2_cbc_encrypt</u>	DES encryption
<u>DES_edc2_cfb64_encrypt</u>	DES encryption
<u>DES_edc2_ofb64_encrypt</u>	DES encryption
<u>DES_edc3_cbc_encrypt</u>	DES encryption
<u>DES_edc3_cbcm_encrypt</u>	DES encryption
<u>DES_edc3_cfb64_encrypt</u>	DES encryption
<u>DES_edc3_ofb64_encrypt</u>	DES encryption
<u>DES_enc_read</u>	DES encryption
<u>DES_enc_write</u>	DES encryption
<u>DES_fcrypt</u>	DES encryption
<u>des</u>	DES encryption
<u>DES_is_weak_key</u>	DES encryption
<u>DES_key_sched</u>	DES encryption
<u>DES_ncbc_encrypt</u>	DES encryption
<u>DES_ofb64_encrypt</u>	DES encryption
<u>DES_ofb_encrypt</u>	DES encryption
<u>DES_pcbc_encrypt</u>	DES encryption
<u>DES_quad_cksum</u>	DES encryption
<u>DES_random_key</u>	DES encryption
<u>des_read_2passwords</u>	Compatibility user interface functions
<u>des_read_password</u>	Compatibility user interface functions
<u>des_read_pw</u>	Compatibility user interface functions
<u>des_read_pw_string</u>	Compatibility user interface functions
<u>DES_set_key_checked</u>	DES encryption
<u>DES_set_key</u>	DES encryption
<u>DES_set_key_unchecked</u>	DES encryption
<u>DES_set_odd_parity</u>	DES encryption
<u>DES_string_to_2keys</u>	DES encryption
<u>DES_string_to_key</u>	DES encryption
<u>DES_xcbc_encrypt</u>	DES encryption
<u>DH_check</u>	generate and check Diffie-Hellman parameters
<u>DH_compute_key</u>	perform Diffie-Hellman key exchange
<u>DH_free</u>	allocate and free DH objects
<u>DH_generate_key</u>	perform Diffie-Hellman key exchange
<u>DH_generate_parameters_ex</u>	generate and check Diffie-Hellman parameters
<u>DH_generate_parameters</u>	generate and check Diffie-Hellman parameters
<u>DH_get_default_method</u>	select DH method
<u>DH_get_ex_data</u>	add application specific data to DH structures
<u>DH_get_ex_new_index</u>	add application specific data to DH structures
<u>dh</u>	Diffie-Hellman key agreement

<u>DH_new</u>	allocate and free DH objects
<u>DH_new_method</u>	select DH method
<u>DH_OpenSSL</u>	select DH method
<u>DHparams_print_fp</u>	print cryptographic parameters
<u>DHparams_print</u>	print cryptographic parameters
<u>DH_set_default_method</u>	select DH method
<u>DH_set_ex_data</u>	add application specific data to DH structures
<u>DH_set_method</u>	select DH method
<u>DH_size</u>	get Diffie-Hellman prime size
<u>DSA_do_sign</u>	raw DSA signature operations
<u>DSA_do_verify</u>	raw DSA signature operations
<u>DSA_dup_DH</u>	create a DH structure out of DSA structure
<u>DSA_free</u>	allocate and free DSA objects
<u>DSA_generate_key</u>	generate DSA key pair
<u>DSA_generate_parameters_ex</u>	generate DSA parameters
<u>DSA_generate_parameters</u>	generate DSA parameters
<u>DSA_get_default_method</u>	select DSA method
<u>DSA_get_ex_data</u>	add application specific data to DSA structures
<u>DSA_get_ex_new_index</u>	add application specific data to DSA structures
<u>dsa</u>	Digital Signature Algorithm
<u>DSA_new</u>	allocate and free DSA objects
<u>DSA_new_method</u>	select DSA method
<u>DSA_OpenSSL</u>	select DSA method
<u>DSAParams_print_fp</u>	print cryptographic parameters
<u>DSAParams_print</u>	print cryptographic parameters
<u>DSA_print_fp</u>	print cryptographic parameters
<u>DSA_print</u>	print cryptographic parameters
<u>DSA_set_default_method</u>	select DSA method
<u>DSA_set_ex_data</u>	add application specific data to DSA structures
<u>DSA_set_method</u>	select DSA method
<u>DSA_SIG_free</u>	allocate and free DSA signature objects
<u>DSA_SIG_new</u>	allocate and free DSA signature objects
<u>DSA_sign</u>	DSA signatures
<u>DSA_sign_setup</u>	DSA signatures
<u>DSA_size</u>	get DSA signature size
<u>DSA_verify</u>	DSA signatures
<u>DTLS_client_method</u>	create a new SSL_CTX object as framework for TLS/SSL enabled functions
<u>DTLS_method</u>	create a new SSL_CTX object as framework for TLS/SSL enabled functions
<u>DTLS_server_method</u>	create a new SSL_CTX object as framework for TLS/SSL enabled functions
<u>DTLSv1_2_client_method</u>	create a new SSL_CTX object as framework for TLS/SSL enabled functions
<u>DTLSv1_2_method</u>	create a new SSL_CTX object as framework for TLS/SSL enabled functions
<u>DTLSv1_2_server_method</u>	create a new SSL_CTX object as framework for TLS/SSL enabled functions

[DTLSv1_client_method](#)

[DTLSv1_method](#)

[DTLSv1_server_method](#)

[ECDSA_do_sign_ex](#)

[ECDSA_do_sign](#)

[ECDSA_do_verify](#)

[ecdsa](#)

[ECDSA_SIG_free](#)

[ECDSA_SIG_new](#)

[ECDSA_sign_ex](#)

[ECDSA_sign](#)

[ECDSA_sign_setup](#)

[ECDSA_size](#)

[ECDSA_verify](#)

[EC_get_builtin_curves](#)

[EC_GF2m_simple_method](#)

[EC_GFp_mont_method](#)

[EC_GFp_nist_method](#)

[EC_GFp_nistp224_method](#)

[EC_GFp_nistp256_method](#)

[EC_GFp_nistp521_method](#)

[EC_GFp_simple_method](#)

[EC_GROUP_check_discriminant](#)

[EC_GROUP_check](#)

[EC_GROUP_clear_free](#)

[EC_GROUP_cmp](#)

[EC_GROUP_copy](#)

[EC_GROUP_dup](#)

[EC_GROUP_free](#)

[EC_GROUP_get0_generator](#)

[EC_GROUP_get0_seed](#)

[EC_GROUP_get_asn1_flag](#)

[EC_GROUP_get_basis_type](#)

[EC_GROUP_get_cofactor](#)

[EC_GROUP_get_curve_GF2m](#)

[EC_GROUP_get_curve_GFp](#)

[EC_GROUP_get_curve_name](#)

[EC_GROUP_get_degree](#)

[EC_GROUP_get_order](#)

[EC_GROUP_get_pentanomial_basis](#)

[EC_GROUP_get_point_conversion_form](#)

[EC_GROUP_get_seed_len](#)

[EC_GROUP_get_trinomial_basis](#)

[EC_GROUP_have_precompute_mult](#)

[EC_GROUP_method_of](#)

create a new SSL_CTX object as framework for TLS/SSL enabled functions

create a new SSL_CTX object as framework for TLS/SSL enabled functions

create a new SSL_CTX object as framework for TLS/SSL enabled functions

Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm

Functions for creating and destroying B objects.

Functions for obtaining B objects.

Functions for obtaining B objects.

Functions for obtaining B objects.

Functions for obtaining B objects.

Functions for obtaining B objects.

Functions for obtaining B objects.

Functions for obtaining B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for creating and destroying B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for creating and destroying B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for creating and destroying B objects.

Functions for creating and destroying B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for manipulating B objects.

Functions for performing mathematical operations and tests on B objects.

Functions for manipulating B objects.

<u>EC_GROUP_new_by_curve_name</u>	Functions for creating and destroying B objects.
<u>EC_GROUP_new_curve_GF2m</u>	Functions for creating and destroying B objects.
<u>EC_GROUP_new_curve_GFP</u>	Functions for creating and destroying B objects.
<u>EC_GROUP_new</u>	Functions for creating and destroying B objects.
<u>EC_GROUP_precompute_mult</u>	Functions for performing mathematical operations and tests on B objects.
<u>EC_GROUP_set_asn1_flag</u>	Functions for manipulating B objects.
<u>EC_GROUP_set_curve_GF2m</u>	Functions for creating and destroying B objects.
<u>EC_GROUP_set_curve_GFP</u>	Functions for creating and destroying B objects.
<u>EC_GROUP_set_curve_name</u>	Functions for manipulating B objects.
<u>EC_GROUP_set_generator</u>	Functions for manipulating B objects.
<u>EC_GROUP_set_point_conversion_form</u>	Functions for manipulating B objects.
<u>EC_GROUP_set_seed</u>	Functions for manipulating B objects.
<u>ec</u>	Elliptic Curve functions
<u>EC_KEY_check_key</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_clear_flags</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_copy</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_dup</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_free</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_generate_key</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_get0_group</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_get0_private_key</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_get0_public_key</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_get_conv_form</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_get_enc_flags</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_get_flags</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_get_key_method_data</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_insert_key_method_data</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_new_by_curve_name</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_new</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_precompute_mult</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_set_asn1_flag</u>	Functions for creating, destroying and manipulating B objects.

<u>EC_KEY_set_conv_form</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_set_enc_flags</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_set_flags</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_set_group</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_set_private_key</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_set_public_key_affine_coordinates</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_set_public_key</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_KEY_up_ref</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_METHOD_get_field_type</u>	Functions for obtaining B objects.
<u>ECPKParameters_print_fp</u>	Functions for decoding and encoding ASN1 representations of elliptic curve entities
<u>ECPKParameters_print</u>	Functions for decoding and encoding ASN1 representations of elliptic curve entities
<u>EC_POINT_add</u>	Functions for performing mathematical operations and tests on B objects.
<u>EC_POINT_bn2point</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_clear_free</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_cmp</u>	Functions for performing mathematical operations and tests on B objects.
<u>EC_POINT_copy</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_dbl</u>	Functions for performing mathematical operations and tests on B objects.
<u>EC_POINT_dup</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_free</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_get_affine_coordinates_GF2m</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_get_affine_coordinates_GFP</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_get_Jprojective_coordinates_GFP</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_hex2point</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_invert</u>	Functions for performing mathematical operations and tests on B objects.
<u>EC_POINT_is_at_infinity</u>	Functions for performing mathematical operations and tests on B objects.
<u>EC_POINT_is_on_curve</u>	Functions for performing mathematical operations and tests on B objects.

<u>EC_POINT_make_affine</u>	Functions for performing mathematical operations and tests on B objects.
<u>EC_POINT_method_of</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_mul</u>	Functions for performing mathematical operations and tests on B objects.
<u>EC_POINT_new</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_oct2point</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_point2bn</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_point2hex</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_point2oct</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_set_affine_coordinates_GF2m</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_set_affine_coordinates_GFP</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_set_compressed_coordinates_GF2m</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_set_compressed_coordinates_GFP</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_set_Jprojective_coordinates</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINT_set_to_infinity</u>	Functions for creating, destroying and manipulating B objects.
<u>EC_POINTS_make_affine</u>	Functions for performing mathematical operations and tests on B objects.
<u>EC_POINTS_mul</u>	Functions for performing mathematical operations and tests on B objects.
<u>ENGINE_add_conf_module</u>	add standard configuration modules
<u>engine</u>	ENGINE cryptographic module support
<u>ERR_add_error_data</u>	record an error
<u>ERR_clear_error</u>	clear the error queue
<u>ERR_error_string</u>	obtain human-readable error message
<u>ERR_error_string_n</u>	obtain human-readable error message
<u>ERR_free_strings</u>	load and free error strings
<u>ERR_func_error_string</u>	obtain human-readable error message
<u>ERR_get_error</u>	obtain error code and data
<u>ERR_get_error_line_data</u>	obtain error code and data
<u>ERR_get_error_line</u>	obtain error code and data
<u>ERR_GET_FUNC</u>	get library, function and reason code
<u>ERR_GET_LIB</u>	get library, function and reason code
<u>ERR_get_next_error_library</u>	load arbitrary error strings
<u>ERR_GET_REASON</u>	get library, function and reason code
<u>err</u>	error codes
<u>ERR_lib_error_string</u>	obtain human-readable error message
<u>ERR_load_crypto_strings</u>	load and free error strings

<u>ERR_load_strings</u>	load arbitrary error strings
<u>ERR_load_UI_strings</u>	New User Interface
<u>ERR_PACK</u>	load arbitrary error strings
<u>ERR_peek_error</u>	obtain error code and data
<u>ERR_peek_error_line_data</u>	obtain error code and data
<u>ERR_peek_error_line</u>	obtain error code and data
<u>ERR_peek_last_error</u>	obtain error code and data
<u>ERR_peek_last_error_line_data</u>	obtain error code and data
<u>ERR_peek_last_error_line</u>	obtain error code and data
<u>ERR_pop_to_mark</u>	set marks and pop errors until mark
<u>ERR_print_errors_fp</u>	print error messages
<u>ERR_print_errors</u>	print error messages
<u>ERR_put_error</u>	record an error
<u>ERR_reason_error_string</u>	obtain human-readable error message
<u>ERR_remove_state</u>	free a thread's error queue
<u>ERR_remove_thread_state</u>	free a thread's error queue
<u>ERR_set_mark</u>	set marks and pop errors until mark
<u>EVP_aes_128_cbc_hmac_sha1</u>	EVP cipher routines
<u>EVP_aes_128_cbc_hmac_sha256</u>	EVP cipher routines
<u>EVP_aes_128_ccm</u>	EVP cipher routines
<u>EVP_aes_128_gcm</u>	EVP cipher routines
<u>EVP_aes_192_ccm</u>	EVP cipher routines
<u>EVP_aes_192_gcm</u>	EVP cipher routines
<u>EVP_aes_256_cbc_hmac_sha1</u>	EVP cipher routines
<u>EVP_aes_256_cbc_hmac_sha256</u>	EVP cipher routines
<u>EVP_aes_256_ccm</u>	EVP cipher routines
<u>EVP_aes_256_gcm</u>	EVP cipher routines
<u>EVP_bf_cbc</u>	EVP cipher routines
<u>EVP_bf_cfb</u>	EVP cipher routines
<u>EVP_bf_ecb</u>	EVP cipher routines
<u>EVP_bf_ofb</u>	EVP cipher routines
<u>EVP_BytesToKey</u>	password based encryption routine
<u>EVP_cast5_cbc</u>	EVP cipher routines
<u>EVP_cast5_cfb</u>	EVP cipher routines
<u>EVP_cast5_ecb</u>	EVP cipher routines
<u>EVP_cast5_ofb</u>	EVP cipher routines
<u>EVP_CIPHER_asn1_to_param</u>	EVP cipher routines
<u>EVP_CIPHER_block_size</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_block_size</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_cipher</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_cleanup</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_ctrl</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_flags</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_get_app_data</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_init</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_iv_length</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_key_length</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_mode</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_nid</u>	EVP cipher routines

<u>EVP_CIPHER_CTX_set_app_data</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_set_key_length</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_set_padding</u>	EVP cipher routines
<u>EVP_CIPHER_CTX_type</u>	EVP cipher routines
<u>EVP_CipherFinal_ex</u>	EVP cipher routines
<u>EVP_CipherFinal</u>	EVP cipher routines
<u>EVP_CIPHER_flags</u>	EVP cipher routines
<u>EVP_CipherInit_ex</u>	EVP cipher routines
<u>EVP_CipherInit</u>	EVP cipher routines
<u>EVP_CIPHER_iv_length</u>	EVP cipher routines
<u>EVP_CIPHER_key_length</u>	EVP cipher routines
<u>EVP_CIPHER_mode</u>	EVP cipher routines
<u>EVP_CIPHER_nid</u>	EVP cipher routines
<u>EVP_CIPHER_param_to_asn1</u>	EVP cipher routines
<u>EVP_CIPHER_type</u>	EVP cipher routines
<u>EVP_CipherUpdate</u>	EVP cipher routines
<u>EVP_cleanup</u>	add algorithms to internal table
<u>EVP_DecodeBlock</u>	EVP base 64 encode/decode routines
<u>EVP_DecodeFinal</u>	EVP base 64 encode/decode routines
<u>EVP_DecodeInit</u>	EVP base 64 encode/decode routines
<u>EVP_DecodeUpdate</u>	EVP base 64 encode/decode routines
<u>EVP_DecryptFinal_ex</u>	EVP cipher routines
<u>EVP_DecryptFinal</u>	EVP cipher routines
<u>EVP_DecryptInit_ex</u>	EVP cipher routines
<u>EVP_DecryptInit</u>	EVP cipher routines
<u>EVP_DecryptUpdate</u>	EVP cipher routines
<u>EVP_des_cbc</u>	EVP cipher routines
<u>EVP_des_cfb</u>	EVP cipher routines
<u>EVP_des_ecb</u>	EVP cipher routines
<u>EVP_des_ede3_cbc</u>	EVP cipher routines
<u>EVP_des_ede3_cfb</u>	EVP cipher routines
<u>EVP_des_ede3</u>	EVP cipher routines
<u>EVP_des_ede3_ofb</u>	EVP cipher routines
<u>EVP_des_ede_cbc</u>	EVP cipher routines
<u>EVP_des_ede_cfb</u>	EVP cipher routines
<u>EVP_des_ede</u>	EVP cipher routines
<u>EVP_des_ede_ofb</u>	EVP cipher routines
<u>EVP_des_ofb</u>	EVP cipher routines
<u>EVP_desx_cbc</u>	EVP cipher routines
<u>EVP_DigestFinal_ex</u>	EVP digest routines
<u>EVP_DigestFinal</u>	EVP digest routines
<u>EVP_DigestInit_ex</u>	EVP digest routines
<u>EVP_DigestInit</u>	EVP digest routines
<u>EVP_DigestSignFinal</u>	EVP signing functions
<u>EVP_DigestSignInit</u>	EVP signing functions
<u>EVP_DigestSignUpdate</u>	EVP signing functions
<u>EVP_DigestUpdate</u>	EVP digest routines
<u>EVP_DigestVerifyFinal</u>	EVP signature verification functions
<u>EVP_DigestVerifyInit</u>	EVP signature verification functions

[EVP_DigestVerifyUpdate](#)
[EVP_dss1](#)
[EVP_dss](#)
[EVP_enc_null](#)
[EVP_EncodeBlock](#)
[EVP_EncodeFinal](#)
[EVP_EncodeInit](#)
[EVP_EncodeUpdate](#)
[EVP_EncryptFinal_ex](#)
[EVP_EncryptFinal](#)
[EVP_EncryptInit_ex](#)
[EVP_EncryptInit](#)
[EVP_EncryptUpdate](#)
[EVP_get_cipherbyname](#)
[EVP_get_cipherbynid](#)
[EVP_get_cipherbyobj](#)
[EVP_get_digestbyname](#)
[EVP_get_digestbynid](#)
[EVP_get_digestbyobj](#)
[evp](#)
[EVP_idea_cbc](#)
[EVP_idea_cfb](#)
[EVP_idea_ecb](#)
[EVP_idea_ofb](#)
[EVP_MAX_MD_SIZE](#)
[EVP_md2](#)
[EVP_md5](#)
[EVP_MD_block_size](#)
[EVP_mdc2](#)
[EVP_MD_CTX_block_size](#)
[EVP_MD_CTX_cleanup](#)
[EVP_MD_CTX_copy_ex](#)
[EVP_MD_CTX_copy](#)
[EVP_MD_CTX_create](#)
[EVP_MD_CTX_destroy](#)
[EVP_MD_CTX_init](#)
[EVP_MD_CTX_md](#)
[EVP_MD_CTX_size](#)
[EVP_MD_CTX_type](#)
[EVP_md_null](#)
[EVP_MD_pkey_type](#)
[EVP_MD_size](#)
[EVP_MD_type](#)
[EVP_OpenFinal](#)
[EVP_OpenInit](#)
[EVP_OpenUpdate](#)
[EVP_PKEYVP_PKEY_CTX_set_app_data](#)
[EVP_PKEY_assign_DH](#)
[EVP_PKEY_assign_DSA](#)

[EVP_PKEY_assign_EC_KEY](#)
[EVP_PKEY_assign_RSA](#)
[EVP_PKEY_cmp](#)
[EVP_PKEY_cmp_parameters](#)
[EVP_PKEY_copy_parameters](#)
[EVP_PKEY_CTX_ctrl](#)
[EVP_PKEY_CTX_ctrl_str](#)
[EVP_PKEY_CTX_dup](#)
[EVP_PKEY_CTX_free](#)
[EVP_PKEY_CTX_get_app_data](#)
[EVP_PKEY_CTX_get_cb](#)
[EVP_PKEY_CTX_get_keygen_info](#)
[EVP_PKEY_CTX_new](#)
[EVP_PKEY_CTX_new_id](#)
[EVP_PKEY_CTX_set_cb](#)
[EVP_PKEY_CTX_set_dh_paramgen_generator](#)
[EVP_PKEY_CTX_set_dh_paramgen_prime_len](#)
[EVP_PKEY_CTX_set_dsa_paramgen_bits](#)
[EVP_PKEY_CTX_set_ec_paramgen_curve_nid](#)
[EVP_PKEY_CTX_set_rsa_keygen_pubexp](#)
[EVP_PKEY_CTX_set_rsa_padding](#)
[EVP_PKEY_CTX_set_rsa_pss_saltlen](#)
[EVP_PKEY_CTX_set_rsa_keygen_bits](#)
[EVP_PKEY_CTX_set_signature_md](#)
[EVP_PKEY_decrypt](#)
[EVP_PKEY_decrypt_init](#)
[EVP_PKEY_derive](#)
[EVP_PKEY_derive_init](#)
[EVP_PKEY_derive_set_peer](#)
[EVP_PKEY_encrypt](#)
[EVP_PKEY_encrypt_init](#)
[EVP_PKEY_free](#)
[EVP_PKEY_get1_DH](#)
[EVP_PKEY_get1_DSA](#)
[EVP_PKEY_get1_EC_KEY](#)
[EVP_PKEY_get1_RSA](#)
[EVP_PKEY_get_default_digest](#)
[EVP_PKEY_get_default_digest_nid](#)
[EVP_PKEY_keygen](#)
[EVP_PKEY_keygen_init](#)
[EVP_PKEY_meth_add0](#)
[EVP_PKEY_meth_copy](#)
[EVP_PKEY_meth_find](#)
[EVP_PKEY_meth_free](#)
[EVP_PKEY_meth_get_cleanup](#)
[EVP_PKEY_meth_get_copy](#)
[EVP_PKEY_meth_get_ctrl](#)
[EVP_PKEY_meth_get_decrypt](#)
[EVP_PKEY_meth_get_derive](#)

EVP_PKEY assignment functions.
EVP_PKEY assignment functions.
public key parameter and comparison functions
public key parameter and comparison functions
public key parameter and comparison functions
algorithm specific control operations
algorithm specific control operations
public key algorithm context functions.
public key algorithm context functions.
key and parameter generation functions
key and parameter generation functions
key and parameter generation functions
public key algorithm context functions.
public key algorithm context functions.
key and parameter generation functions
algorithm specific control operations
algorithm specific control operations
algorithm specific control operations
algorithm specific control operations
algorithm specific control operations
algorithm specific control operations
algorithm specific control operations
algorithm specific control operations
algorithm specific control operations
decrypt using a public key algorithm
decrypt using a public key algorithm
derive public key algorithm shared secret.
derive public key algorithm shared secret.
derive public key algorithm shared secret.
encrypt using a public key algorithm
encrypt using a public key algorithm
private key allocation functions.
EVP_PKEY assignment functions.
EVP_PKEY assignment functions.
EVP_PKEY assignment functions.
EVP_PKEY assignment functions.
get default signature digest
get default signature digest
key and parameter generation functions
key and parameter generation functions
manipulating EVP_PKEY_METHOD structure
manipulating EVP_PKEY_METHOD structure
manipulating EVP_PKEY_METHOD structure
manipulating EVP_PKEY_METHOD structure
manipulating EVP_PKEY_METHOD structure
manipulating EVP_PKEY_METHOD structure
manipulating EVP_PKEY_METHOD structure
manipulating EVP_PKEY_METHOD structure
manipulating EVP_PKEY_METHOD structure
manipulating EVP_PKEY_METHOD structure

[EVP_PKEY_meth_get_encrypt](#)
[EVP_PKEY_meth_get_init](#)
[EVP_PKEY_meth_get_keygen](#)
[EVP_PKEY_meth_get_paramgen](#)
[EVP_PKEY_meth_get_signctx](#)
[EVP_PKEY_meth_get_sign](#)
[EVP_PKEY_meth_get_verifyctx](#)
[EVP_PKEY_meth_get_verify](#)
[EVP_PKEY_meth_get_verify_recover](#)
[EVP_PKEY_meth_new](#)
[EVP_PKEY_METHOD](#)
[EVP_PKEY_meth_set_cleanup](#)
[EVP_PKEY_meth_set_copy](#)
[EVP_PKEY_meth_set_ctrl](#)
[EVP_PKEY_meth_set_decrypt](#)
[EVP_PKEY_meth_set_derive](#)
[EVP_PKEY_meth_set_encrypt](#)
[EVP_PKEY_meth_set_init](#)
[EVP_PKEY_meth_set_keygen](#)
[EVP_PKEY_meth_set_paramgen](#)
[EVP_PKEY_meth_set_signctx](#)
[EVP_PKEY_meth_set_sign](#)
[EVP_PKEY_meth_set_verifyctx](#)
[EVP_PKEY_meth_set_verify](#)
[EVP_PKEY_meth_set_verify_recover](#)
[EVP_PKEY_missing_parameters](#)
[EVP_PKEY_new](#)
[EVP_PKEY_paramgen](#)
[EVP_PKEY_paramgen_init](#)
[EVP_PKEY_print_params](#)
[EVP_PKEY_print_private](#)
[EVP_PKEY_print_public](#)
[EVP_PKEY_set1_DH](#)
[EVP_PKEY_set1_DSA](#)
[EVP_PKEY_set1_EC_KEY](#)
[EVP_PKEY_set1_RSA](#)
[EVP_PKEY_sign](#)
[EVP_PKEY_sign_init](#)
[EVP_PKEY_type](#)
[EVP_PKEY_verify](#)
[EVP_PKEY_verify_init](#)
[EVP_PKEY_verify_recover](#)
[EVP_PKEY_verify_recover_init](#)
[EVP_rc2_40_cbc](#)
[EVP_rc2_64_cbc](#)
[EVP_rc2_cbc](#)
[EVP_rc2_cfb](#)
[EVP_rc2_ecb](#)
[EVP_rc2_ofb](#)

EVP_rc4_40	EVP cipher routines
EVP_rc4_hmac_md5	EVP cipher routines
EVP_rc4	EVP cipher routines
EVP_rc5_32_12_16_cbc	EVP cipher routines
EVP_rc5_32_12_16_cfb	EVP cipher routines
EVP_rc5_32_12_16_ecb	EVP cipher routines
EVP_rc5_32_12_16_ofb	EVP cipher routines
EVP_ripemd160	EVP digest routines
EVP_SealFinal	EVP envelope encryption
EVP_SealInit	EVP envelope encryption
EVP_SealUpdate	EVP envelope encryption
EVP_sha1	EVP digest routines
EVP_sha224	EVP digest routines
EVP_sha256	EVP digest routines
EVP_sha384	EVP digest routines
EVP_sha512	EVP digest routines
EVP_sha	EVP digest routines
EVP_SignFinal	EVP signing functions
EVP_SignInit_ex	EVP signing functions
EVP_SignInit	EVP signing functions
EVP_SignUpdate	EVP signing functions
EVP_VerifyFinal	EVP signature verification functions
EVP_VerifyInit	EVP signature verification functions
EVP_VerifyUpdate	EVP signature verification functions
HMAC_cleanup	HMAC message authentication code
HMAC_CTX_cleanup	HMAC message authentication code
HMAC_CTX_init	HMAC message authentication code
HMAC_Final	HMAC message authentication code
hmac	HMAC message authentication code
HMAC	HMAC message authentication code
HMAC_Init_ex	HMAC message authentication code
HMAC_Init	HMAC message authentication code
HMAC_Update	HMAC message authentication code
i2d_ASN1_OBJECT	ASN1 OBJECT IDENTIFIER functions
i2d_CMS_bio_stream	output CMS_ContentInfo structure in BER format.
i2d_CMS_ContentInfo	CMS ContentInfo functions
i2d_DHparams	PKCS#3 DH parameter functions.
i2d_DSAParams	DSA key encoding and parsing functions.
i2d_DSAPrivateKey	DSA key encoding and parsing functions.
i2d_DSA_PUBKEY	DSA key encoding and parsing functions.
i2d_DSAPublicKey	DSA key encoding and parsing functions.
i2d_DSA_SIG	DSA key encoding and parsing functions.
i2d_ECDSA_SIG	Elliptic Curve Digital Signature Algorithm
i2d_ECCKParameters_bio	Functions for decoding and encoding ASN1 representations of elliptic curve entities
i2d_ECCKParameters_fp	Functions for decoding and encoding ASN1 representations of elliptic curve entities
i2d_ECCKParameters	Functions for decoding and encoding ASN1 representations of elliptic curve entities

[i2d_ECPrivateKey](#)

[i2d_Netscape_RSA](#)

[i2d_PKCS7_bio_stream](#)

[i2d_PKCS8PrivateKey_bio](#)

[i2d_PKCS8PrivateKey_fp](#)

[i2d_PKCS8PrivateKey_nid_bio](#)

[i2d_PKCS8PrivateKey_nid_fp](#)

[i2d_PrivateKey](#)

[i2d_RSAPrivateKey](#)

[i2d_RSA_PUBKEY](#)

[i2d_RSAPublicKey](#)

[i2d_SSL_SESSION](#)

[i2d_X509_ALGOR](#)

[i2d_X509_bio](#)

[i2d_X509_CRL_bio](#)

[i2d_X509_CRL_fp](#)

[i2d_X509_CRL](#)

[i2d_X509_fp](#)

[i2d_X509](#)

[i2d_X509_NAME](#)

[i2d_X509_REQ_bio](#)

[i2d_X509_REQ_fp](#)

[i2d_X509_REQ](#)

[i2d_X509_SIG](#)

[lhash](#)

[lh_delete](#)

[lh_doall_arg](#)

[lh_doall](#)

[lh_error](#)

[lh_free](#)

[lh_insert](#)

[lh_new](#)

[lh_node_stats_bio](#)

[lh_node_stats](#)

[lh_node_usage_stats_bio](#)

[lh_node_usage_stats](#)

[lh_retrieve](#)

[lh_stats_bio](#)

[lh_stats](#)

[MD2_Final](#)

[MD2](#)

[MD2_Init](#)

[MD2_Update](#)

[MD4_Final](#)

[MD4](#)

[MD4_Init](#)

Encode and decode functions for saving and reading EC_KEY structures

RSA public and private key encoding functions. output PKCS7 structure in BER format.

PKCS#8 format private key functions

PKCS#8 format private key functions

PKCS#8 format private key functions

PKCS#8 format private key functions

decode and encode functions for reading and saving EVP_PKEY structures.

RSA public and private key encoding functions.

RSA public and private key encoding functions.

RSA public and private key encoding functions. convert SSL_SESSION object from/to ASN1 representation

AlgorithmIdentifier functions.

X509 encode and decode functions

PKCS#10 certificate request functions.

PKCS#10 certificate request functions.

PKCS#10 certificate request functions.

X509 encode and decode functions

X509 encode and decode functions

X509_NAME encoding functions

PKCS#10 certificate request functions.

PKCS#10 certificate request functions.

PKCS#10 certificate request functions.

DigestInfo functions.

dynamic hash table

dynamic hash table

dynamic hash table

dynamic hash table

dynamic hash table

dynamic hash table

dynamic hash table

dynamic hash table

LHASH statistics

LHASH statistics

LHASH statistics

LHASH statistics

dynamic hash table

LHASH statistics

LHASH statistics

MD2, MD4, and MD5 hash functions

MD2, MD4, and MD5 hash functions

MD2, MD4, and MD5 hash functions

MD2, MD4, and MD5 hash functions

MD2, MD4, and MD5 hash functions

MD2, MD4, and MD5 hash functions

MD2, MD4, and MD5 hash functions

MD4_Update	MD2, MD4, and MD5 hash functions
MD5_Final	MD2, MD4, and MD5 hash functions
md5	MD2, MD4, and MD5 hash functions
MD5	MD2, MD4, and MD5 hash functions
MD5_Init	MD2, MD4, and MD5 hash functions
MD5_Update	MD2, MD4, and MD5 hash functions
MDC2_Final	MDC2 hash function
mdc2	MDC2 hash function
MDC2	MDC2 hash function
MDC2_Init	MDC2 hash function
MDC2_Update	MDC2 hash function
OBJ_cleanup	ASN1 object utility functions
OBJ_cmp	ASN1 object utility functions
OBJ_create	ASN1 object utility functions
OBJ_dup	ASN1 object utility functions
OBJ_ln2nid	ASN1 object utility functions
OBJ_nid2ln	ASN1 object utility functions
OBJ_nid2obj	ASN1 object utility functions
OBJ_nid2sn	ASN1 object utility functions
OBJ_obj2nid	ASN1 object utility functions
OBJ_obj2txt	ASN1 object utility functions
OBJ_sn2nid	ASN1 object utility functions
OBJ_txt2nid	ASN1 object utility functions
OBJ_txt2obj	ASN1 object utility functions
OpenSSL_add_all_algorithms	add algorithms to internal table
OpenSSL_add_all_ciphers	add algorithms to internal table
OpenSSL_add_all_digests	add algorithms to internal table
OpenSSL_add_ssl_algorithms	initialize SSL library by registering algorithms
OPENSSL_Applink	glue between OpenSSL BIO and Win32 compiler run-time
OPENSSL_config	simple OpenSSL configuration functions
OPENSSL_ia32cap	the IA-32 processor capabilities vector
OPENSSL_ia32cap_loc	the IA-32 processor capabilities vector
OPENSSL_instrument_bus2	instrument references to memory bus
OPENSSL_instrument_bus	instrument references to memory bus
OPENSSL_load_builtin_modules	add standard configuration modules
OPENSSL_no_config	simple OpenSSL configuration functions
OPENSSL_VERSION_NUMBER	get OpenSSL version number
OPENSSL_VERSION_TEXT	get OpenSSL version number
pem	PEM routines
PEM	PEM routines
PEM_read_bio_DHparams	PEM routines
PEM_read_bio_DSAParams	PEM routines
PEM_read_bio_DSAPrivateKey	PEM routines
PEM_read_bio_DSA_PUBKEY	PEM routines
PEM_read_bio_NETSCAPE_CERT_SEQUENCE	PEM routines
PEM_read_bio_PKCS7	PEM routines
PEM_read_bio_PrivateKey	PEM routines
PEM_read_bio_PUBKEY	PEM routines

PEM_read_bio_RSAPrivateKey	PEM routines
PEM_read_bio_RSA_PUBKEY	PEM routines
PEM_read_bio_RSAPublicKey	PEM routines
PEM_read_bio_X509_AUX	PEM routines
PEM_read_bio_X509_CRL	PEM routines
PEM_read_bio_X509	PEM routines
PEM_read_bio_X509_REQ	PEM routines
PEM_read_DHparams	PEM routines
PEM_read_DSAParams	PEM routines
PEM_read_DSAPrivateKey	PEM routines
PEM_read_DSA_PUBKEY	PEM routines
PEM_read_NETSCAPE_CERT_SEQUENCE	PEM routines
PEM_read_PKCS7	PEM routines
PEM_read_PrivateKey	PEM routines
PEM_read_PUBKEY	PEM routines
PEM_read_RSAPrivateKey	PEM routines
PEM_read_RSA_PUBKEY	PEM routines
PEM_read_RSAPublicKey	PEM routines
PEM_read_X509_AUX	PEM routines
PEM_read_X509_CRL	PEM routines
PEM_read_X509	PEM routines
PEM_read_X509_REQ	PEM routines
PEM_write_bio_CMS_stream	output CMS_ContentInfo structure in PEM format.
PEM_write_bio_DHparams	PEM routines
PEM_write_bio_DSAParams	PEM routines
PEM_write_bio_DSAPrivateKey	PEM routines
PEM_write_bio_DSA_PUBKEY	PEM routines
PEM_write_bio_NETSCAPE_CERT_SEQUENCE	PEM routines
PEM_write_bio_PKCS7	PEM routines
PEM_write_bio_PKCS7_stream	output PKCS7 structure in PEM format.
PEM_write_bio_PKCS8PrivateKey	PEM routines
PEM_write_bio_PKCS8PrivateKey_nid	PEM routines
PEM_write_bio_PrivateKey	PEM routines
PEM_write_bio_PUBKEY	PEM routines
PEM_write_bio_RSAPrivateKey	PEM routines
PEM_write_bio_RSA_PUBKEY	PEM routines
PEM_write_bio_RSAPublicKey	PEM routines
PEM_write_bio_X509_AUX	PEM routines
PEM_write_bio_X509_CRL	PEM routines
PEM_write_bio_X509	PEM routines
PEM_write_bio_X509_REQ	PEM routines
PEM_write_bio_X509_REQ_NEW	PEM routines
PEM_write_DHparams	PEM routines
PEM_write_DSAParams	PEM routines
PEM_write_DSAPrivateKey	PEM routines
PEM_write_DSA_PUBKEY	PEM routines
PEM_write_NETSCAPE_CERT_SEQUENCE	PEM routines
PEM_write_PKCS7	PEM routines
PEM_write_PKCS8PrivateKey	PEM routines

<u>PEM_write_PKCS8PrivateKey_nid</u>	PEM routines
<u>PEM_write_PrivateKey</u>	PEM routines
<u>PEM_write_PUBKEY</u>	PEM routines
<u>PEM_write_RSAPrivateKey</u>	PEM routines
<u>PEM_write_RSA_PUBKEY</u>	PEM routines
<u>PEM_write_RSAPublicKey</u>	PEM routines
<u>PEM_write_X509_AUX</u>	PEM routines
<u>PEM_write_X509_CRL</u>	PEM routines
<u>PEM_write_X509</u>	PEM routines
<u>PEM_write_X509_REQ</u>	PEM routines
<u>PEM_write_X509_REQ_NEW</u>	PEM routines
<u>PKCS12_create</u>	create a PKCS#12 structure
<u>PKCS12_parse</u>	parse a PKCS#12 structure
<u>PKCS7_decrypt</u>	decrypt content from a PKCS#7 envelopedData structure
<u>PKCS7_encrypt</u>	create a PKCS#7 envelopedData structure
<u>PKCS7_get0_signers</u>	verify a PKCS#7 signedData structure
<u>PKCS7_sign_add_signer</u>	add a signer PKCS7 signed data structure.
<u>PKCS7_sign</u>	create a PKCS#7 signedData structure
<u>PKCS7_verify</u>	verify a PKCS#7 signedData structure
<u>RAND_add</u>	add entropy to the PRNG
<u>RAND_bytes</u>	generate random data
<u>RAND_cleanup</u>	erase the PRNG state
<u>RAND_egd_bytes</u>	query entropy gathering daemon
<u>RAND_egd</u>	query entropy gathering daemon
<u>RAND_event</u>	add entropy to the PRNG
<u>RAND_file_name</u>	PRNG seed file
<u>RAND_get_rand_method</u>	select RAND method
<u>rand</u>	pseudo-random number generator
<u>RAND_load_file</u>	PRNG seed file
<u>RAND_pseudo_bytes</u>	generate random data
<u>RAND_query_egd_bytes</u>	query entropy gathering daemon
<u>RAND_screen</u>	add entropy to the PRNG
<u>RAND_seed</u>	add entropy to the PRNG
<u>RAND_set_rand_method</u>	select RAND method
<u>RAND_SSLeay</u>	select RAND method
<u>RAND_status</u>	add entropy to the PRNG
<u>RAND_write_file</u>	PRNG seed file
<u>rc4</u>	RC4 encryption
<u>RC4</u>	RC4 encryption
<u>RC4_set_key</u>	RC4 encryption
<u>RIPEMD160_Final</u>	RIPEMD-160 hash function
<u>RIPEMD160</u>	RIPEMD-160 hash function
<u>RIPEMD160_Init</u>	RIPEMD-160 hash function
<u>RIPEMD160_Update</u>	RIPEMD-160 hash function
<u>ripemd</u>	RIPEMD-160 hash function
<u>RSA_blinding_off</u>	protect the RSA operation from timing attacks
<u>RSA_blinding_on</u>	protect the RSA operation from timing attacks
<u>RSA_check_key</u>	validate private RSA keys

RSA_flags	select RSA method
RSA_free	allocate and free RSA objects
RSA_generate_key_ex	generate RSA key pair
RSA_generate_key	generate RSA key pair
RSA_get_default_method	select RSA method
RSA_get_ex_data	add application specific data to RSA structures
RSA_get_ex_new_index	add application specific data to RSA structures
RSA_get_method	select RSA method
rsa	RSA public key cryptosystem
RSA_new	allocate and free RSA objects
RSA_new_method	select RSA method
RSA_null_method	select RSA method
RSA_padding_add_none	asymmetric encryption padding
RSA_padding_add_PKCS1_OAEP	asymmetric encryption padding
RSA_padding_add_PKCS1_type_1	asymmetric encryption padding
RSA_padding_add_PKCS1_type_2	asymmetric encryption padding
RSA_padding_add_SSLv23	asymmetric encryption padding
RSA_padding_check_none	asymmetric encryption padding
RSA_padding_check_PKCS1_OAEP	asymmetric encryption padding
RSA_padding_check_PKCS1_type_1	asymmetric encryption padding
RSA_padding_check_PKCS1_type_2	asymmetric encryption padding
RSA_padding_check_SSLv23	asymmetric encryption padding
RSA_PKCS1_SSLeay	select RSA method
RSA_print_fp	print cryptographic parameters
RSA_print	print cryptographic parameters
RSA_private_decrypt	RSA public key cryptography
RSA_private_encrypt	low level signature operations
RSA_public_decrypt	low level signature operations
RSA_public_encrypt	RSA public key cryptography
RSA_set_default_method	select RSA method
RSA_set_ex_data	add application specific data to RSA structures
RSA_set_method	select RSA method
RSA_sign_ASN1_OCTET_STRING	RSA signatures
RSA_sign	RSA signatures
RSA_size	get RSA modulus size
RSA_verify_ASN1_OCTET_STRING	RSA signatures
RSA_verify	RSA signatures
SHA1_Final	Secure Hash Algorithm
SHA1	Secure Hash Algorithm
SHA1_Init	Secure Hash Algorithm
SHA1_Update	Secure Hash Algorithm
SHA224_Final	Secure Hash Algorithm
SHA224	Secure Hash Algorithm
SHA224_Init	Secure Hash Algorithm
SHA224_Update	Secure Hash Algorithm
SHA256_Final	Secure Hash Algorithm
SHA256	Secure Hash Algorithm
SHA256_Init	Secure Hash Algorithm
SHA256_Update	Secure Hash Algorithm

<u>SHA384_Final</u>	Secure Hash Algorithm
<u>SHA384</u>	Secure Hash Algorithm
<u>SHA384_Init</u>	Secure Hash Algorithm
<u>SHA384_Update</u>	Secure Hash Algorithm
<u>SHA512_Final</u>	Secure Hash Algorithm
<u>SHA512</u>	Secure Hash Algorithm
<u>SHA512_Init</u>	Secure Hash Algorithm
<u>SHA512_Update</u>	Secure Hash Algorithm
<u>sha</u>	Secure Hash Algorithm
<u>SMIME_read_CMS</u>	parse S/MIME message.
<u>SMIME_read_PKCS7</u>	parse S/MIME message.
<u>SMIME_write_CMS</u>	convert CMS structure to S/MIME format.
<u>SMIME_write_PKCS7</u>	convert PKCS#7 structure to S/MIME format.
<u>SSL_accept</u>	wait for a TLS/SSL client to initiate a TLS/SSL handshake
<u>SSL_add0_chain_cert</u>	extra chain certificate processing
<u>SSL_add1_chain_cert</u>	extra chain certificate processing
<u>SSL_add_client_CA</u>	set list of CAs sent to the client when requesting a client certificate
<u>SSL_add_session</u>	manipulate session cache
<u>SSL_alert_desc_string</u>	get textual description of alert information
<u>SSL_alert_desc_string_long</u>	get textual description of alert information
<u>SSL_alert_type_string</u>	get textual description of alert information
<u>SSL_alert_type_string_long</u>	get textual description of alert information
<u>SSL_build_cert_chain</u>	extra chain certificate processing
<u>SSL_callback_ctrl</u>	internal handling functions for SSL_CTX and SSL objects
<u>SSL_check_chain</u>	check certificate chain suitability
<u>SSL_check_private_key</u>	load certificate and key data
<u>SSL_CIPHER_description</u>	get SSL_CIPHER properties
<u>SSL_CIPHER_get_bits</u>	get SSL_CIPHER properties
<u>SSL_CIPHER_get_name</u>	get SSL_CIPHER properties
<u>SSL_CIPHER_get_version</u>	get SSL_CIPHER properties
<u>SSL_clear_chain_certs</u>	extra chain certificate processing
<u>SSL_clear</u>	reset SSL object to allow another connection
<u>SSL_clear_options</u>	manipulate SSL options
<u>SSL_COMP_add_compression_method</u>	handle SSL/TLS integrated compression methods
<u>SSL_COMP_free_compression_methods</u>	handle SSL/TLS integrated compression methods
<u>SSL_CONF_cmd_argv</u>	SSL configuration command line processing.
<u>SSL_CONF_cmd</u>	send configuration command
<u>SSL_CONF_CTX_clear_flags</u>	Set of clear SSL configuration context flags
<u>SSL_CONF_CTX_free</u>	SSL configuration allocation functions
<u>SSL_CONF_CTX_new</u>	SSL configuration allocation functions
<u>SSL_CONF_CTX_set1_prefix</u>	Set configuration context command prefix
<u>SSL_CONF_CTX_set_flags</u>	Set of clear SSL configuration context flags
<u>SSL_CONF_CTX_set_ssl_ctx</u>	set context to configure
<u>SSL_CONF_CTX_set_ssl</u>	set context to configure
<u>SSL_connect</u>	initiate the TLS/SSL handshake with an TLS/SSL server

<u>SSL_ctrl</u>	internal handling functions for SSL_CTX and SSL objects
<u>SSL_CTX_add0_chain_cert</u>	extra chain certificate processing
<u>SSL_CTX_add1_chain_cert</u>	extra chain certificate processing
<u>SSL_CTX_add_client_CA</u>	set list of CAs sent to the client when requesting a client certificate
<u>SSL_CTX_add_client_custom_ext</u>	custom TLS extension handling
<u>SSL_CTX_add_extra_chain_cert</u>	add or clear extra chain certificates
<u>SSL_CTX_add_server_custom_ext</u>	custom TLS extension handling
<u>SSL_CTX_add_session</u>	manipulate session cache
<u>SSL_CTX_build_cert_chain</u>	extra chain certificate processing
<u>SSL_CTX_callback_ctrl</u>	internal handling functions for SSL_CTX and SSL objects
<u>SSL_CTX_check_private_key</u>	load certificate and key data
<u>SSL_CTX_clear_chain_certs</u>	extra chain certificate processing
<u>SSL_CTX_clear_extra_chain_certs</u>	add or clear extra chain certificates
<u>SSL_CTX_clear_options</u>	manipulate SSL options
<u>SSL_CTX_ctrl</u>	internal handling functions for SSL_CTX and SSL objects
<u>SSL_CTX_flush_sessions</u>	remove expired sessions
<u>SSL_CTX_free</u>	free an allocated SSL_CTX object
<u>SSL_CTX_get0_chain_certs</u>	extra chain certificate processing
<u>SSL_CTX_get0_param</u>	get and set verification parameters
<u>SSL_CTX_get_cert_store</u>	manipulate X509 certificate verification storage
<u>SSL_CTX_get_client_CA_list</u>	get list of client CAs
<u>SSL_CTX_get_client_cert_cb</u>	handle client certificate callback function
<u>SSL_CTX_get_default_read_ahead</u>	manage whether to read as many input bytes as possible
<u>SSL_CTX_get_ex_data</u>	internal application specific data functions
<u>SSL_CTX_get_ex_new_index</u>	internal application specific data functions
<u>SSL_CTX_get_info_callback</u>	handle information callback for SSL connections
<u>SSL_CTX_get_max_cert_list</u>	manipulate allowed for the peer's certificate chain
<u>SSL_CTX_get_mode</u>	manipulate SSL engine mode
<u>SSL_CTX_get_options</u>	manipulate SSL options
<u>SSL_CTX_get_quiet_shutdown</u>	manipulate shutdown behaviour
<u>SSL_CTX_get_read_ahead</u>	manage whether to read as many input bytes as possible
<u>SSL_CTX_get_session_cache_mode</u>	enable/disable session caching
<u>SSL_CTX_get_timeout</u>	manipulate timeout values for session caching
<u>SSL_CTX_get_verify_callback</u>	get currently set verification parameters
<u>SSL_CTX_get_verify_depth</u>	get currently set verification parameters
<u>SSL_CTX_get_verify_mode</u>	get currently set verification parameters
<u>SSL_CTX_load_verify_locations</u>	set default locations for trusted CA certificates
<u>SSL_CTX_need_tmp_rsa</u>	handle RSA keys for ephemeral key exchange
<u>SSL_CTX_new</u>	create a new SSL_CTX object as framework for TLS/SSL enabled functions
<u>SSL_CTX_remove_session</u>	manipulate session cache
<u>SSL_CTX_select_current_cert</u>	extra chain certificate processing
<u>SSL_CTX_sess_accept_good</u>	obtain session cache statistics
<u>SSL_CTX_sess_accept</u>	obtain session cache statistics
<u>SSL_CTX_sess_accept_renegotiate</u>	obtain session cache statistics

<u>SSL_CTX_sess_cache_full</u>	obtain session cache statistics
<u>SSL_CTX_sess_cb_hits</u>	obtain session cache statistics
<u>SSL_CTX_sess_connect_good</u>	obtain session cache statistics
<u>SSL_CTX_sess_connect</u>	obtain session cache statistics
<u>SSL_CTX_sess_connect_renegotiate</u>	obtain session cache statistics
<u>SSL_CTX_sess_get_cache_size</u>	manipulate session cache size
<u>SSL_CTX_sess_get_get_cb</u>	provide callback functions for server side external session caching
<u>SSL_CTX_sess_get_new_cb</u>	provide callback functions for server side external session caching
<u>SSL_CTX_sess_get_remove_cb</u>	provide callback functions for server side external session caching
<u>SSL_CTX_sess_hits</u>	obtain session cache statistics
<u>SSL_CTX_sessions</u>	access internal session cache
<u>SSL_CTX_sess_misses</u>	obtain session cache statistics
<u>SSL_CTX_sess_number</u>	obtain session cache statistics
<u>SSL_CTX_sess_set_cache_size</u>	manipulate session cache size
<u>SSL_CTX_sess_set_get_cb</u>	provide callback functions for server side external session caching
<u>SSL_CTX_sess_set_new_cb</u>	provide callback functions for server side external session caching
<u>SSL_CTX_sess_set_remove_cb</u>	provide callback functions for server side external session caching
<u>SSL_CTX_sess_timeouts</u>	obtain session cache statistics
<u>SSL_CTX_set0_chain_cert_store</u>	set certificate verification or chain store
<u>SSL_CTX_set0_chain</u>	extra chain certificate processing
<u>SSL_CTX_set0_verify_cert_store</u>	set certificate verification or chain store
<u>SSL_CTX_set1_chain_cert_store</u>	set certificate verification or chain store
<u>SSL_CTX_set1_chain</u>	extra chain certificate processing
<u>SSL_CTX_set1_curves</u>	EC supported curve functions
<u>SSL_CTX_set1_curves_list</u>	EC supported curve functions
<u>SSL_CTX_set1_param</u>	get and set verification parameters
<u>SSL_CTX_set1_verify_cert_store</u>	set certificate verification or chain store
<u>SSL_CTX_set_alpn_protos</u>	handle application layer protocol negotiation (ALPN)
<u>SSL_CTX_set_alpn_select_cb</u>	handle application layer protocol negotiation (ALPN)
<u>SSL_CTX_set_cert_cb</u>	handle certificate callback function
<u>SSL_CTX_set_cert_store</u>	manipulate X509 certificate verification storage
<u>SSL_CTX_set_cert_verify_callback</u>	set peer certificate verification procedure
<u>SSL_CTX_set_cipher_list</u>	choose list of available SSL_CIPHERs
<u>SSL_CTX_set_client_CA_list</u>	set list of CAs sent to the client when requesting a client certificate
<u>SSL_CTX_set_client_cert_cb</u>	handle client certificate callback function
<u>SSL_CTX_set_current_cert</u>	extra chain certificate processing
<u>SSL_CTX_set_custom_cli_ext</u>	custom TLS extension handling
<u>SSL_CTX_set_default_passwd_cb</u>	set passwd callback for encrypted PEM file handling
<u>SSL_CTX_set_default_passwd_cb_userdata</u>	set passwd callback for encrypted PEM file handling
<u>SSL_CTX_set_default_read_ahead</u>	manage whether to read as many input bytes as possible
<u>SSL_CTX_set_ecdh_auto</u>	EC supported curve functions
<u>SSL_CTX_set_ex_data</u>	internal application specific data functions

<u>SSL_CTX_set_generate_session_id</u>	manipulate generation of SSL session IDs (server only)
<u>SSL_CTX_set_info_callback</u>	handle information callback for SSL connections
<u>SSL_CTX_set_max_cert_list</u>	manipulate allowed for the peer's certificate chain
<u>SSL_CTX_set_mode</u>	manipulate SSL engine mode
<u>SSL_CTX_set_msg_callback_arg</u>	install callback for observing protocol messages
<u>SSL_CTX_set_msg_callback</u>	install callback for observing protocol messages
<u>SSL_CTX_set_options</u>	manipulate SSL options
<u>SSL_CTX_set_psk_client_callback</u>	set PSK client callback
<u>SSL_CTX_set_psk_server_callback</u>	set PSK identity hint to use
<u>SSL_CTX_set_quiet_shutdown</u>	manipulate shutdown behaviour
<u>SSL_CTX_set_read_ahead</u>	manage whether to read as many input bytes as possible
<u>SSL_CTX_set_session_cache_mode</u>	enable/disable session caching
<u>SSL_CTX_set_session_id_context</u>	set context within which session can be reused (server side only)
<u>SSL_CTX_set_ssl_version</u>	choose a new TLS/SSL method
<u>SSL_CTX_set_timeout</u>	manipulate timeout values for session caching
<u>SSL_CTX_set_tlsext_servername_arg</u>	handle server name indication (SNI)
<u>SSL_CTX_set_tlsext_servername_callback</u>	handle server name indication (SNI)
<u>SSL_CTX_set_tlsext_status_arg</u>	OCSP Certificate Status Request functions
<u>SSL_CTX_set_tlsext_status_cb</u>	OCSP Certificate Status Request functions
<u>SSL_CTX_set_tlsext_ticket_key_cb</u>	set a callback for session ticket processing
<u>SSL_CTX_set_tmp_dh_callback</u>	handle DH keys for ephemeral key exchange
<u>SSL_CTX_set_tmp_dh</u>	handle DH keys for ephemeral key exchange
<u>SSL_CTX_set_tmp_rsa_callback</u>	handle RSA keys for ephemeral key exchange
<u>SSL_CTX_set_tmp_rsa</u>	handle RSA keys for ephemeral key exchange
<u>SSL_CTX_set_verify_depth</u>	set peer certificate verification parameters
<u>SSL_CTX_set_verify</u>	set peer certificate verification parameters
<u>SSL_CTX_use_certificate_ASN1</u>	load certificate and key data
<u>SSL_CTX_use_certificate_chain_file</u>	load certificate and key data
<u>SSL_CTX_use_certificate_file</u>	load certificate and key data
<u>SSL_CTX_use_certificate</u>	load certificate and key data
<u>SSL_CTX_use_PrivateKey_ASN1</u>	load certificate and key data
<u>SSL_CTX_use_PrivateKey_file</u>	load certificate and key data
<u>SSL_CTX_use_PrivateKey</u>	load certificate and key data
<u>SSL_CTX_use_psk_identity_hint</u>	set PSK identity hint to use
<u>SSL_CTX_use_RSAPrivateKey_ASN1</u>	load certificate and key data
<u>SSL_CTX_use_RSAPrivateKey_file</u>	load certificate and key data
<u>SSL_CTX_use_RSAPrivateKey</u>	load certificate and key data
<u>SSL_CTX_use_serverinfo_file</u>	use serverinfo extension
<u>SSL_CTX_use_serverinfo</u>	use serverinfo extension
<u>SSL_do_handshake</u>	perform a TLS/SSL handshake
<u>SSL_load_error_strings</u>	initialize SSL library by registering algorithms
<u>SSL_get_version</u>	get OpenSSL version number
<u>SSL_get0_version</u>	retrieve version/build information about OpenSSL library
<u>SSL_get0_key</u>	obtain keying material for application use
<u>SSL_remove_expired_sessions</u>	remove expired sessions
<u>SSL_free</u>	free an allocated SSL structure
<u>SSL_get0_alpn_selected</u>	handle application layer protocol negotiation (ALPN)

<u>SSL_get0_chain_certs</u>	extra chain certificate processing
<u>SSL_get0_param</u>	get and set verification parameters
<u>SSL_get1_curves</u>	EC supported curve functions
<u>SSL_get_accept_state</u>	prepare SSL object to work in client or server mode
<u>SSL_get_cipher_bits</u>	get SSL_CIPHER of a connection
<u>SSL_get_cipher</u>	get SSL_CIPHER of a connection
<u>SSL_get_cipher_list</u>	get list of available SSL_CIPHERs
<u>SSL_get_cipher_name</u>	get SSL_CIPHER of a connection
<u>SSL_get_ciphers</u>	get list of available SSL_CIPHERs
<u>SSL_get_cipher_version</u>	get SSL_CIPHER of a connection
<u>SSL_get_client_CA_list</u>	get list of client CAs
<u>SSL_get_current_cipher</u>	get SSL_CIPHER of a connection
<u>SSL_get_default_timeout</u>	get default session timeout value
<u>SSL_get_error</u>	obtain result code for TLS/SSL I/O operation
<u>SSL_get_ex_data</u>	internal application specific data functions
<u>SSL_get_ex_data_X509_STORE_CTX_idx</u>	get ex_data index to access SSL structure from X509_STORE_CTX
<u>SSL_get_ex_new_index</u>	internal application specific data functions
<u>SSL_get_fd</u>	get file descriptor linked to an SSL object
<u>SSL_get_info_callback</u>	handle information callback for SSL connections
<u>SSL_get_max_cert_list</u>	manipulate allowed for the peer's certificate chain
<u>SSL_get_mode</u>	manipulate SSL engine mode
<u>SSL_get_msg_callback_arg</u>	install callback for observing protocol messages
<u>SSL_get_options</u>	manipulate SSL options
<u>SSL_get_peer_cert_chain</u>	get the X509 certificate chain of the peer
<u>SSL_get_peer_certificate</u>	get the X509 certificate of the peer
<u>SSL_get_psk_identity_hint</u>	get PSK client identity and hint
<u>SSL_get_psk_identity</u>	get PSK client identity and hint
<u>SSL_get_quiet_shutdown</u>	manipulate shutdown behaviour
<u>SSL_get_rbio</u>	get BIO linked to an SSL object
<u>SSL_get_read_ahead</u>	manage whether to read as many input bytes as possible
<u>SSL_get_secure_renegotiation_support</u>	manipulate SSL options
<u>SSL_get_servername</u>	handle server name indication (SNI)
<u>SSL_get_servername_type</u>	handle server name indication (SNI)
<u>SSL_get_session</u>	retrieve TLS/SSL session data
<u>SSL_get_shared_ciphers</u>	get list of available SSL_CIPHERs
<u>SSL_get_shared_curve</u>	EC supported curve functions
<u>SSL_get_shutdown</u>	manipulate shutdown state of an SSL connection
<u>SSL_get_SSL_CTX</u>	get the SSL_CTX from which an SSL is created
<u>SSL_get_ssl_method</u>	choose a new TLS/SSL method
<u>SSL_get_tlsext_status_ocsp_resp</u>	OCSP Certificate Status Request functions
<u>SSL_get_verify_callback</u>	get currently set verification parameters
<u>SSL_get_verify_depth</u>	get currently set verification parameters
<u>SSL_get_verify_mode</u>	get currently set verification parameters
<u>SSL_get_verify_result</u>	get result of peer certificate verification
<u>SSL_get_version</u>	get the protocol version of a connection.
<u>SSL_has_matching_session_id</u>	manipulate generation of SSL session IDs (server only)
<u>ssl</u>	OpenSSL SSL/TLS library
<u>SSL</u>	OpenSSL SSL/TLS library

<u>SSL_library_init</u>	initialize SSL library by registering algorithms
<u>SSL_load_client_CA_file</u>	load certificate names from file
<u>SSL_load_error_strings</u>	load and free error strings
<u>SSL_need_tmp_rsa</u>	handle RSA keys for ephemeral key exchange
<u>SSL_new</u>	create a new SSL structure for a connection
<u>SSL_pending</u>	obtain number of readable bytes buffered in an SSL object
<u>SSL_read</u>	read bytes from a TLS/SSL connection.
<u>SSL_remove_session</u>	manipulate session cache
<u>SSL_rstate_string</u>	get textual description of state of an SSL object during read operation
<u>SSL_rstate_string_long</u>	get textual description of state of an SSL object during read operation
<u>SSL_select_current_cert</u>	extra chain certificate processing
<u>SSL_select_next_proto</u>	handle application layer protocol negotiation (ALPN)
<u>SSL_SESSION_free</u>	free an allocated SSL_SESSION structure
<u>SSL_SESSION_get_ex_data</u>	internal application specific data functions
<u>SSL_SESSION_get_ex_new_index</u>	internal application specific data functions
<u>SSL_SESSION_get_time</u>	retrieve and manipulate session time and timeout settings
<u>SSL_SESSION_get_timeout</u>	retrieve and manipulate session time and timeout settings
<u>SSL_session_reused</u>	query whether a reused session was negotiated during handshake
<u>SSL_SESSION_set_ex_data</u>	internal application specific data functions
<u>SSL_SESSION_set_time</u>	retrieve and manipulate session time and timeout settings
<u>SSL_SESSION_set_timeout</u>	retrieve and manipulate session time and timeout settings
<u>SSL_set0_chain_cert_store</u>	set certificate verification or chain store
<u>SSL_set0_chain</u>	extra chain certificate processing
<u>SSL_set0_verify_cert_store</u>	set certificate verification or chain store
<u>SSL_set1_chain_cert_store</u>	set certificate verification or chain store
<u>SSL_set1_chain</u>	extra chain certificate processing
<u>SSL_set1_curves</u>	EC supported curve functions
<u>SSL_set1_curves_list</u>	EC supported curve functions
<u>SSL_set1_param</u>	get and set verification parameters
<u>SSL_set1_verify_cert_store</u>	set certificate verification or chain store
<u>SSL_set_alpn_protos</u>	handle application layer protocol negotiation (ALPN)
<u>SSL_set_bio</u>	connect the SSL object with a BIO
<u>SSL_set_cert_cb</u>	handle certificate callback function
<u>SSL_set_cipher_list</u>	choose list of available SSL_CIPHERs
<u>SSL_set_client_CA_list</u>	set list of CAs sent to the client when requesting a client certificate
<u>SSL_set_connect_state</u>	prepare SSL object to work in client or server mode
<u>SSL_set_current_cert</u>	extra chain certificate processing
<u>SSL_set_ecdh_auto</u>	EC supported curve functions
<u>SSL_set_ex_data</u>	internal application specific data functions
<u>SSL_set_fd</u>	connect the SSL object with a file descriptor

<u>SSL_set_generate_session_id</u>	manipulate generation of SSL session IDs (server only)
<u>SSL_set_info_callback</u>	handle information callback for SSL connections
<u>SSL_set_max_cert_list</u>	manipulate allowed for the peer's certificate chain
<u>SSL_set_mode</u>	manipulate SSL engine mode
<u>SSL_set_msg_callback</u>	install callback for observing protocol messages
<u>SSL_set_options</u>	manipulate SSL options
<u>SSL_set_psk_client_callback</u>	set PSK client callback
<u>SSL_set_psk_server_callback</u>	set PSK identity hint to use
<u>SSL_set_quiet_shutdown</u>	manipulate shutdown behaviour
<u>SSL_set_read_ahead</u>	manage whether to read as many input bytes as possible
<u>SSL_set_session</u>	set a TLS/SSL session to be used during TLS/SSL connect
<u>SSL_set_session_id_context</u>	set context within which session can be reused (server side only)
<u>SSL_set_shutdown</u>	manipulate shutdown state of an SSL connection
<u>SSL_set_ssl_method</u>	choose a new TLS/SSL method
<u>SSL_set_tlsext_status_ocsp_resp</u>	OCSP Certificate Status Request functions
<u>SSL_set_tlsext_status_type</u>	OCSP Certificate Status Request functions
<u>SSL_set_tmp_dh_callback</u>	handle DH keys for ephemeral key exchange
<u>SSL_set_tmp_dh</u>	handle DH keys for ephemeral key exchange
<u>SSL_set_tmp_rsa_callback</u>	handle RSA keys for ephemeral key exchange
<u>SSL_set_tmp_rsa</u>	handle RSA keys for ephemeral key exchange
<u>SSL_set_verify_depth</u>	set peer certificate verification parameters
<u>SSL_set_verify</u>	set peer certificate verification parameters
<u>SSL_set_verify_result</u>	override result of peer certificate verification
<u>SSL_shutdown</u>	shut down a TLS/SSL connection
<u>SSL_state_string</u>	get textual description of state of an SSL object
<u>SSL_state_string_long</u>	get textual description of state of an SSL object
<u>SSL_use_certificate_ASN1</u>	load certificate and key data
<u>SSL_use_certificate_file</u>	load certificate and key data
<u>SSL_use_certificate</u>	load certificate and key data
<u>SSL_use_PrivateKey_ASN1</u>	load certificate and key data
<u>SSL_use_PrivateKey_file</u>	load certificate and key data
<u>SSL_use_PrivateKey</u>	load certificate and key data
<u>SSL_use_psk_identity_hint</u>	set PSK identity hint to use
<u>SSL_use_RSAPrivateKey_ASN1</u>	load certificate and key data
<u>SSL_use_RSAPrivateKey_file</u>	load certificate and key data
<u>SSL_use_RSAPrivateKey</u>	load certificate and key data
<u>SSLv23_client_method</u>	create a new SSL_CTX object as framework for TLS/SSL enabled functions
<u>SSLv23_method</u>	create a new SSL_CTX object as framework for TLS/SSL enabled functions
<u>SSLv23_server_method</u>	create a new SSL_CTX object as framework for TLS/SSL enabled functions
<u>SSLv2_client_method</u>	create a new SSL_CTX object as framework for TLS/SSL enabled functions
<u>SSLv2_method</u>	create a new SSL_CTX object as framework for TLS/SSL enabled functions

SSLv2_server_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
SSLv3_client_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
SSLv3_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
SSLv3_server_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
SSL_want	obtain state information TLS/SSL I/O operation
SSL_want_nothing	obtain state information TLS/SSL I/O operation
SSL_want_read	obtain state information TLS/SSL I/O operation
SSL_want_write	obtain state information TLS/SSL I/O operation
SSL_want_x509_lookup	obtain state information TLS/SSL I/O operation
SSL_write	write bytes to a TLS/SSL connection.
threads	OpenSSL thread support
TLSv1_1_client_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
TLSv1_1_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
TLSv1_1_server_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
TLSv1_2_client_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
TLSv1_2_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
TLSv1_2_server_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
TLSv1_client_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
TLSv1_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
TLSv1_server_method	create a new SSL_CTX object as framework for TLS/SSL enabled functions
UI_add_error_string	New User Interface
UI_add_info_string	New User Interface
UI_add_input_boolean	New User Interface
UI_add_input_string	New User Interface
UI_add_user_data	New User Interface
UI_add_verify_string	New User Interface
ui_compat	Compatibility user interface functions
UI_construct_prompt	New User Interface
UI_ctrl	New User Interface
UI_dup_error_string	New User Interface
UI_dup_info_string	New User Interface
UI_dup_input_boolean	New User Interface
UI_dup_input_string	New User Interface
UI_dup_verify_string	New User Interface
UI_free	New User Interface
UI_get0_result	New User Interface
UI_get0_user_data	New User Interface

UI_get_default_method	New User Interface
UI_get_method	New User Interface
ui	New User Interface
UI_new	New User Interface
UI_new_method	New User Interface
UI_OpenSSL	New User Interface
UI_process	New User Interface
UI_set_default_method	New User Interface
UI_set_method	New User Interface
X509_check_email	X.509 certificate matching
X509_check_host	X.509 certificate matching
X509_check_ip_asc	X.509 certificate matching
X509_check_ip	X.509 certificate matching
X509_check_private_key	check the consistency of a private key with the public key in an X509 certificate or certificate request
X509_cmp_time	X509 time functions
X509_free	X509 certificate ASN1 allocation functions
x509	X.509 certificate handling
X509_NAME_add_entry_by_NID	X509_NAME modification functions
X509_NAME_add_entry_by_OBJ	X509_NAME modification functions
X509_NAME_add_entry_by_txt	X509_NAME modification functions
X509_NAME_add_entry	X509_NAME modification functions
X509_NAME_delete_entry	X509_NAME modification functions
X509_NAME_entry_count	X509_NAME lookup and enumeration functions
X509_NAME_ENTRY_create_by_NID	X509_NAME_ENTRY utility functions
X509_NAME_ENTRY_create_by_OBJ	X509_NAME_ENTRY utility functions
X509_NAME_ENTRY_create_by_txt	X509_NAME_ENTRY utility functions
X509_NAME_ENTRY_get_data	X509_NAME_ENTRY utility functions
X509_NAME_ENTRY_get_object	X509_NAME_ENTRY utility functions
X509_NAME_ENTRY_set_data	X509_NAME_ENTRY utility functions
X509_NAME_ENTRY_set_object	X509_NAME_ENTRY utility functions
X509_NAME_get_entry	X509_NAME lookup and enumeration functions
X509_NAME_get_index_by_NID	X509_NAME lookup and enumeration functions
X509_NAME_get_index_by_OBJ	X509_NAME lookup and enumeration functions
X509_NAME_get_text_by_NID	X509_NAME lookup and enumeration functions
X509_NAME_get_text_by_OBJ	X509_NAME lookup and enumeration functions
X509_NAME_online	X509_NAME printing routines.
X509_NAME_print_ex_fp	X509_NAME printing routines.
X509_NAME_print_ex	X509_NAME printing routines.
X509_NAME_print	X509_NAME printing routines.
X509_new	X509 certificate ASN1 allocation functions
X509_REQ_check_private_key	check the consistency of a private key with the public key in an X509 certificate or certificate request
X509_STORE_CTX_cleanup	X509_STORE_CTX initialisation
X509_STORE_CTX_free	X509_STORE_CTX initialisation
X509_STORE_CTX_get0_param	get or set certificate verification status information
X509_STORE_CTX_get1_chain	get or set certificate verification status information
X509_STORE_CTX_get_current_cert	get or set certificate verification status information
X509_STORE_CTX_get_error_depth	get or set certificate verification status information

X509_STORE_CTX_get_error	get or set certificate verification status information
X509_STORE_CTX_get_ex_data	add application specific data to X509_STORE_CTX structures
X509_STORE_CTX_get_ex_new_index	add application specific data to X509_STORE_CTX structures
X509_STORE_CTX_init	X509_STORE_CTX initialisation
X509_STORE_CTX_new	X509_STORE_CTX initialisation
X509_STORE_CTX_set0_crls	X509_STORE_CTX initialisation
X509_STORE_CTX_set0_param	X509_STORE_CTX initialisation
X509_STORE_CTX_set_cert	X509_STORE_CTX initialisation
X509_STORE_CTX_set_chain	X509_STORE_CTX initialisation
X509_STORE_CTX_set_default	X509_STORE_CTX initialisation
X509_STORE_CTX_set_error	get or set certificate verification status information
X509_STORE_CTX_set_ex_data	add application specific data to X509_STORE_CTX structures
X509_STORE_CTX_set_verify_cb	set verification callback
X509_STORE_CTX_trusted_stack	X509_STORE_CTX initialisation
X509_STORE_set_verify_cb_func	set verification callback
X509_STORE_set_verify_cb	set verification callback
X509_verify_cert_error_string	get or set certificate verification status information
X509_verify_cert	discover and verify X509 certifiecte chain
X509_VERIFY_PARAM_add0_policy	X509 verification parameters
X509_VERIFY_PARAM_add1_host	X509 verification parameters
X509_VERIFY_PARAM_clear_flags	X509 verification parameters
X509_VERIFY_PARAM_get0_peername	X509 verification parameters
X509_VERIFY_PARAM_get_depth	X509 verification parameters
X509_VERIFY_PARAM_get_flags	X509 verification parameters
X509_VERIFY_PARAM_set1_email	X509 verification parameters
X509_VERIFY_PARAM_set1_host	X509 verification parameters
X509_VERIFY_PARAM_set1_ip_asc	X509 verification parameters
X509_VERIFY_PARAM_set1_ip	X509 verification parameters
X509_VERIFY_PARAM_set1_policies	X509 verification parameters
X509_VERIFY_PARAM_set_depth	X509 verification parameters
X509_VERIFY_PARAM_set_flags	X509 verification parameters
X509_VERIFY_PARAM_set_hostflags	X509 verification parameters
X509_VERIFY_PARAM_set_purpose	X509 verification parameters
X509_VERIFY_PARAM_set_time	X509 verification parameters
X509_VERIFY_PARAM_set_trust	X509 verification parameters

You are here:

[Home](#) : [Documentation](#) : [Manpages](#) : [1.0.2](#)

[Sitemap](#)

[Manpages](#)

- [3.1](#)
- [3.0](#)

- [1.1.1](#)
- [1.0.2](#)

Please report problems with this website to webmaster at openssl.org.

Copyright © 1999-2023, OpenSSL Project Authors. All Rights Reserved.

Cryptography and SSL/TLS Toolkit

Search
Navigate... ▼

- [Home](#)
- [Blog](#)
- [Downloads](#)
- [Docs](#)
- [News](#)
- [Roadmap](#)
- [Policies](#)
- [Community](#)
- [Support](#)

RSA_generate_key

NAME

RSA_generate_key_ex, RSA_generate_key - generate RSA key pair

SYNOPSIS

```
#include <openssl/rsa.h>

int RSA_generate_key_ex(RSA *rsa, int bits, BIGNUM *e, BN_GENCB *cb);
```

Deprecated:

```
RSA *RSA_generate_key(int num, unsigned long e,
    void (*callback)(int,int,void *), void *cb_arg);
```

DESCRIPTION

RSA_generate_key_ex() generates a key pair and stores it in the **RSA** structure provided in **rsa**. The pseudo-random number generator must be seeded prior to calling RSA_generate_key_ex().

The modulus size will be of length **bits**, and the public exponent will be **e**. Key sizes with **num** < 1024 should be considered insecure. The exponent is an odd number, typically 3, 17 or 65537.

A callback function may be used to provide feedback about the progress of the key generation. If **cb** is not **NULL**, it will be called as follows using the BN_GENCB_call() function described on the [BN_generate_prime\(3\)](#) page.

- While a random prime number is generated, it is called as described in [BN_generate_prime\(3\)](#).

- When the n-th randomly generated prime is rejected as not suitable for the key, **BN_GENCB_call(cb, 2, n)** is called.
- When a random p has been found with p-1 relatively prime to e, it is called as **BN_GENCB_call(cb, 3, 0)**.

The process is then repeated for prime q with **BN_GENCB_call(cb, 3, 1)**.

`RSA_generate_key` is deprecated (new applications should use `RSA_generate_key_ex` instead).

`RSA_generate_key` works in the same way as `RSA_generate_key_ex` except it uses "old style" call backs. See [BN_generate_prime\(3\)](#) for further details.

RETURN VALUE

If key generation fails, `RSA_generate_key()` returns **NULL**.

The error codes can be obtained by [ERR_get_error\(3\)](#).

BUGS

BN_GENCB_call(cb, 2, x) is used with two different meanings.

`RSA_generate_key()` goes into an infinite loop for illegal input values.

SEE ALSO

[ERR_get_error\(3\)](#), [rand\(3\)](#), [rsa\(3\)](#), [RSA_free\(3\)](#), [BN_generate_prime\(3\)](#).

HISTORY

The **cb_arg** argument was added in SSLeay 0.9.0.

You are here: [Home](#) : [Docs](#) : [Manpages](#) : [1.0.2](#) : [man3](#) : [RSA_generate_key](#)
[Sitemap](#)

[1.0.2 manpages](#)

- [Commands](#)
- [Libraries](#)
- [File Formats](#)
- [Overviews](#)

This manpage

- [master version](#)
- [3.1 version](#)
- [3.0 version](#)
- [1.1.1 version](#)

Please report problems with this website to webmaster at openssl.org.

Copyright © 1999-2023 The OpenSSL Project Authors. All Rights Reserved.