NAME

crypto - OpenSSL cryptographic library

SYNOPSIS

DESCRIPTION

The OpenSSL **crypto** library implements a wide range of cryptographic algorithms used in various Internet standards. The services provided by this library are used by the OpenSSL implementations of SSL, TLS and S/MIME, and they have also been used to implement SSH, OpenPGP, and other cryptographic standards.

OVERVIEW

libcrypto consists of a number of sub-libraries that implement the individual algorithms.

The functionality includes symmetric encryption, public key cryptography and key agreement, certificate handling, cryptographic hash functions and a cryptographic pseudo-random number generator.

SYMMETRIC CIPHERS

blowfish(3), *cast(3)*, *des(3)*, *idea(3)*, *rc2(3)*, *rc4(3)*, *rc5(3)*

PUBLIC KEY CRYPTOGRAPHY AND KEY AGREEMENT

dsa(3), *dh(3)*, *rsa(3)*

CERTIFICATES

x509(3), *x509v3(3)*

AUTHENTICATION CODES, HASH FUNCTIONS

hmac(3), *md2(3)*, *md4(3)*, *md5(3)*, *mdc2(3)*, *ripemd(3)*, *sha(3)*

AUXILIARY FUNCTIONS

err(3), *threads(3)*, *rand(3)*, *OPENSSL_VERSION_NUMBER(3)*

INPUT/OUTPUT, DATA ENCODING

asn1(3), *bio(3)*, *evp(3)*, *pem(3)*, *pkcs7(3)*, *pkcs12(3)*

INTERNAL FUNCTIONS

bn(3), *buffer(3)*, *ec(3)*, *lhash(3)*, *objects(3)*, *stack(3)*, *txt_db(3)*

NOTES

Some of the newer functions follow a naming convention using the numbers **0** and **1**. For example the functions:

```
int X509_CRL_add0_revoked(X509_CRL *crl, X509_REVOKED *rev);
int X509_add1_trust_object(X509 *x, ASN1_OBJECT *obj);
```

The **0** version uses the supplied structure pointer directly in the parent and it will be freed up when the parent is freed. In the above example **crl** would be freed but **rev** would not.

The **1** function uses a copy of the supplied structure pointer (or in some cases increases its link count) in the parent and so both (**x** and **obj** above) should be freed up.

SEE ALSO

openssl(1), *ssl(3)*