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, cast, des, idea, rc2, rc4, rc5

PUBLIC KEY CRYPTOGRAPHY AND KEY AGREEMENT

> dsa, dh, rsa

CERTIFICATES

> x509, x509v3

AUTHENTICATION CODES, HASH FUNCTIONS

> hmac, md2, md4, md5, mdc2, ripemd, sha

AUXILIARY FUNCTIONS

err, threads, rand, OPENSSL_VERSION_NUMBER

INPUT/OUTPUT, DATA ENCODING

asn1, bio, evp, pem, pkcs7, pkcs12

INTERNAL FUNCTIONS

bn, buffer, ec, lhash, objects, stack, txt_db

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, ssl