

NAME

OCSP_cert_to_id, OCSP_cert_id_new, OCSP_CERTID_free, OCSP_id_issuer_cmp, OCSP_id_cmp, OCSP_id_get0_info - OCSP certificate ID utility functions

SYNOPSIS

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

```
OCSP_CERTID *OCSP_cert_to_id(const EVP_MD *dgst,
                             X509 *subject, X509 *issuer);
```

```
OCSP_CERTID *OCSP_cert_id_new(const EVP_MD *dgst,
                              X509_NAME *issuerName,
                              ASN1_BIT_STRING *issuerKey,
                              ASN1_INTEGER *serialNumber);
```

```
void OCSP_CERTID_free(OCSP_CERTID *id);
```

```
int OCSP_id_issuer_cmp(const OCSP_CERTID *a, const OCSP_CERTID *b);
```

```
int OCSP_id_cmp(const OCSP_CERTID *a, const OCSP_CERTID *b);
```

```
int OCSP_id_get0_info(ASN1_OCTET_STRING **piNameHash, ASN1_OBJECT **pmd,
                     ASN1_OCTET_STRING **pikeyHash,
                     ASN1_INTEGER **pserial, OCSP_CERTID *cid);
```

DESCRIPTION

OCSP_cert_to_id() creates and returns a new **OCSP_CERTID** structure using message digest **dgst** for certificate **subject** with issuer **issuer**. If **dgst** is **NULL** then SHA1 is used.

OCSP_cert_id_new() creates and returns a new **OCSP_CERTID** using **dgst** and issuer name **issuerName**, issuer key hash **issuerKey** and serial number **serialNumber**.

OCSP_CERTID_free() frees up **id**.

OCSP_id_cmp() compares **OCSP_CERTID a** and **b**.

OCSP_id_issuer_cmp() compares only the issuer name of **OCSP_CERTID a** and **b**.

OCSP_id_get0_info() returns the issuer name hash, hash OID, issuer key hash and serial number contained in **cid**. If any of the values are not required the corresponding parameter can be set to **NULL**.

RETURN VALUES

OCSP_cert_to_id() and **OCSP_cert_id_new()** return either a pointer to a valid **OCSP_CERTID** structure or **NULL** if an error occurred.

OCSP_id_cmp() and **OCSP_id_issuer_cmp()** returns zero for a match and nonzero otherwise.

OCSP_CERTID_free() does not return a value.

OCSP_id_get0_info() returns 1 for success and 0 for failure.

NOTES

OCSP clients will typically only use **OCSP_cert_to_id()** or **OCSP_cert_id_new()**: the other functions are used by responder applications.

The values returned by **OCSP_id_get0_info()** are internal pointers and **MUST NOT** be freed up by an application: they will be freed when the corresponding **OCSP_CERTID** structure is freed.

SEE ALSO

crypto(7), **OCSP_request_add1_nonce(3)**, **OCSP_REQUEST_new(3)**, **OCSP_resp_find_status(3)**, **OCSP_response_status(3)**, **OCSP_sendreq_new(3)**

COPYRIGHT

Copyright 2015-2016 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.