

**NAME**

hx509 revokation checking functions -

**Functions**

```
int hx509_revoke_init (hx509_context context, hx509_revoke_ctx *ctx)
void hx509_revoke_free (hx509_revoke_ctx *ctx)
int hx509_revoke_add_ocsp (hx509_context context, hx509_revoke_ctx ctx, const char *path)
int hx509_revoke_add_crl (hx509_context context, hx509_revoke_ctx ctx, const char *path)
int hx509_revoke_verify (hx509_context context, hx509_revoke_ctx ctx, hx509_certs certs, time_t now,
hx509_cert cert, hx509_cert parent_cert)
int hx509_ocsp_request (hx509_context context, hx509_certs reqcerts, hx509_certs pool, hx509_cert
signer, const AlgorithmIdentifier *digest, heim_octet_string *request, heim_octet_string *nonce)
int hx509_revoke_ocsp_print (hx509_context context, const char *path, FILE *out)
```

**Detailed Description**

See the **Revocation methods** for description and examples.

**Function Documentation**

```
int hx509_ocsp_request (hx509_context context, hx509_certs reqcerts, hx509_certs pool, hx509_cert
signer, const AlgorithmIdentifier * digest, heim_octet_string * request, heim_octet_string * nonce)
```

Create an OCSP request for a set of certificates.

**Parameters:**

*context* a hx509 context  
*reqcerts* list of certificates to request ocsp data for  
*pool* certificate pool to use when signing  
*signer* certificate to use to sign the request  
*digest* the signing algorithm in the request, if NULL use the default signature algorithm,  
*request* the encoded request, free with free\_heim\_octet\_string().  
*nonce* nonce in the request, free with free\_heim\_octet\_string().

**Returns:**

An hx509 error code, see **hx509\_get\_error\_string()**.

```
int hx509_revoke_add_crl (hx509_context context, hx509_revoke_ctx ctx, const char * path)
```

Add a CRL file to the revokation context.

**Parameters:**

*context* hx509 context  
*ctx* hx509 revokation context

*path* path to file that is going to be added to the context.

**Returns:**

An hx509 error code, see **hx509\_get\_error\_string()**.

**int hx509\_revoke\_add\_ocsp (hx509\_context context, hx509\_revoke\_ctx ctx, const char \* path)**

Add a OCSP file to the revokation context.

**Parameters:**

*context* hx509 context

*ctx* hx509 revokation context

*path* path to file that is going to be added to the context.

**Returns:**

An hx509 error code, see **hx509\_get\_error\_string()**.

**void hx509\_revoke\_free (hx509\_revoke\_ctx \* ctx)**

Free a hx509 revokation context.

**Parameters:**

*ctx* context to be freed

**int hx509\_revoke\_init (hx509\_context context, hx509\_revoke\_ctx \* ctx)**

Allocate a revokation context. Free with **hx509\_revoke\_free()**.

**Parameters:**

*context* A hx509 context.

*ctx* returns a newly allocated revokation context.

**Returns:**

An hx509 error code, see **hx509\_get\_error\_string()**.

**int hx509\_revoke\_ocsp\_print (hx509\_context context, const char \* path, FILE \* out)**

Print the OCSP reply stored in a file.

**Parameters:**

*context* a hx509 context

*path* path to a file with a OCSP reply

*out* the out FILE descriptor to print the reply on

**Returns:**

An hx509 error code, see **hx509\_get\_error\_string()**.

**int hx509\_revoke\_verify (hx509\_context context, hx509\_revoke\_ctx ctx, hx509\_certs certs, time\_t now, hx509\_cert cert, hx509\_cert parent\_cert)**

Check that a certificate is not expired according to a revocation context. Also need the parent certificate to the check OCSP parent identifier.

**Parameters:**

*context* hx509 context

*ctx* hx509 revokation context

*certs*

*now*

*cert*

*parent\_cert*

**Returns:**

An hx509 error code, see **hx509\_get\_error\_string()**.