

**NAME**

X509\_LOOKUP, X509\_LOOKUP\_TYPE, X509\_LOOKUP\_new, X509\_LOOKUP\_free, X509\_LOOKUP\_init, X509\_LOOKUP\_shutdown, X509\_LOOKUP\_set\_method\_data, X509\_LOOKUP\_get\_method\_data, X509\_LOOKUP\_ctrl\_ex, X509\_LOOKUP\_ctrl, X509\_LOOKUP\_load\_file\_ex, X509\_LOOKUP\_load\_file, X509\_LOOKUP\_add\_dir, X509\_LOOKUP\_add\_store\_ex, X509\_LOOKUP\_add\_store, X509\_LOOKUP\_load\_store\_ex, X509\_LOOKUP\_load\_store, X509\_LOOKUP\_get\_store, X509\_LOOKUP\_by\_subject\_ex, X509\_LOOKUP\_by\_subject, X509\_LOOKUP\_by\_issuer\_serial, X509\_LOOKUP\_by\_fingerprint, X509\_LOOKUP\_by\_alias - OpenSSL certificate lookup mechanisms

**SYNOPSIS**

```
#include <openssl/x509_vfy.h>
```

```
typedef x509_lookup_st X509_LOOKUP;
```

```
typedef enum X509_LOOKUP_TYPE;
```

```
X509_LOOKUP *X509_LOOKUP_new(X509_LOOKUP_METHOD *method);
```

```
int X509_LOOKUP_init(X509_LOOKUP *ctx);
```

```
int X509_LOOKUP_shutdown(X509_LOOKUP *ctx);
```

```
void X509_LOOKUP_free(X509_LOOKUP *ctx);
```

```
int X509_LOOKUP_set_method_data(X509_LOOKUP *ctx, void *data);
```

```
void *X509_LOOKUP_get_method_data(const X509_LOOKUP *ctx);
```

```
int X509_LOOKUP_ctrl_ex(X509_LOOKUP *ctx, int cmd, const char *argc, long argl, char **ret, OSSL_LIB_CTX *libctx, const char *propq);
```

```
int X509_LOOKUP_ctrl(X509_LOOKUP *ctx, int cmd, const char *argc, long argl, char **ret);
```

```
int X509_LOOKUP_load_file_ex(X509_LOOKUP *ctx, char *name, long type, OSSL_LIB_CTX *libctx, const char *propq);
```

```
int X509_LOOKUP_load_file(X509_LOOKUP *ctx, char *name, long type);
```

```
int X509_LOOKUP_load_file_ex(X509_LOOKUP *ctx, char *name, long type, OSSL_LIB_CTX *libctx, const char *propq);
```

```
int X509_LOOKUP_add_dir(X509_LOOKUP *ctx, char *name, long type);
```

```
int X509_LOOKUP_add_store_ex(X509_LOOKUP *ctx, char *uri, OSSL_LIB_CTX *libctx, const char *propq);
```

```
int X509_LOOKUP_add_store(X509_LOOKUP *ctx, char *uri);
```

```
int X509_LOOKUP_load_store_ex(X509_LOOKUP *ctx, char *uri, OSSL_LIB_CTX *libctx, const char *propq);
```

```
int X509_LOOKUP_load_store(X509_LOOKUP *ctx, char *uri);

X509_STORE *X509_LOOKUP_get_store(const X509_LOOKUP *ctx);

int X509_LOOKUP_by_subject_ex(X509_LOOKUP *ctx, X509_LOOKUP_TYPE type,
                             const X509_NAME *name, X509_OBJECT *ret,
                             OSSL_LIB_CTX *libctx, const char *propq);
int X509_LOOKUP_by_subject(X509_LOOKUP *ctx, X509_LOOKUP_TYPE type,
                             const X509_NAME *name, X509_OBJECT *ret);
int X509_LOOKUP_by_issuer_serial(X509_LOOKUP *ctx, X509_LOOKUP_TYPE type,
                                 const X509_NAME *name,
                                 const ASN1_INTEGER *serial, X509_OBJECT *ret);
int X509_LOOKUP_by_fingerprint(X509_LOOKUP *ctx, X509_LOOKUP_TYPE type,
                                const unsigned char *bytes, int len,
                                X509_OBJECT *ret);
int X509_LOOKUP_by_alias(X509_LOOKUP *ctx, X509_LOOKUP_TYPE type,
                          const char *str, int len, X509_OBJECT *ret);
```

## DESCRIPTION

The **X509\_LOOKUP** structure holds the information needed to look up certificates and CRLs according to an associated **X509\_LOOKUP\_METHOD**(3). Multiple **X509\_LOOKUP** instances can be added to an **X509\_STORE**(3) to enable lookup in that store.

**X509\_LOOKUP\_new**() creates a new **X509\_LOOKUP** using the given lookup *method*. It can also be created by calling **X509\_STORE\_add\_lookup**(3), which will associate a **X509\_STORE** with the lookup mechanism.

**X509\_LOOKUP\_init**() initializes the internal state and resources as needed by the given **X509\_LOOKUP** to do its work.

**X509\_LOOKUP\_shutdown**() tears down the internal state and resources of the given **X509\_LOOKUP**.

**X509\_LOOKUP\_free**() destructs the given **X509\_LOOKUP**.

**X509\_LOOKUP\_set\_method\_data**() and **X509\_LOOKUP\_get\_method\_data**() associates and retrieves a pointer to application data to and from the given **X509\_LOOKUP**, respectively.

**X509\_LOOKUP\_ctrl\_ex**() is used to set or get additional data to or from a **X509\_LOOKUP** structure or its associated **X509\_LOOKUP\_METHOD**(3). The arguments of the control command are passed via *argc* and *argl*, its return value via *\*ret*. The library context *libctx* and property query *propq* are used

when fetching algorithms from providers. The meaning of the arguments depends on the *cmd* number of the control command. In general, this function is not called directly, but wrapped by a macro call, see below. The control *cmds* known to OpenSSL are discussed in more depth in "Control Commands".

**X509\_LOOKUP\_ctrl()** is similar to **X509\_LOOKUP\_ctrl\_ex()** but uses NULL for the library context *libctx* and property query *propq*.

**X509\_LOOKUP\_load\_file\_ex()** passes a filename to be loaded immediately into the associated **X509\_STORE**. The library context *libctx* and property query *propq* are used when fetching algorithms from providers. *type* indicates what type of object is expected. This can only be used with a lookup using the implementation **X509\_LOOKUP\_file(3)**.

**X509\_LOOKUP\_load\_file()** is similar to **X509\_LOOKUP\_load\_file\_ex()** but uses NULL for the library context *libctx* and property query *propq*.

**X509\_LOOKUP\_add\_dir()** passes a directory specification from which certificates and CRLs are loaded on demand into the associated **X509\_STORE**. *type* indicates what type of object is expected. This can only be used with a lookup using the implementation **X509\_LOOKUP\_hash\_dir(3)**.

**X509\_LOOKUP\_add\_store\_ex()** passes a URI for a directory-like structure from which containers with certificates and CRLs are loaded on demand into the associated **X509\_STORE**. The library context *libctx* and property query *propq* are used when fetching algorithms from providers.

**X509\_LOOKUP\_add\_store()** is similar to **X509\_LOOKUP\_add\_store\_ex()** but uses NULL for the library context *libctx* and property query *propq*.

**X509\_LOOKUP\_load\_store\_ex()** passes a URI for a single container from which certificates and CRLs are immediately loaded into the associated **X509\_STORE**. The library context *libctx* and property query *propq* are used when fetching algorithms from providers. These functions can only be used with a lookup using the implementation **X509\_LOOKUP\_store(3)**.

**X509\_LOOKUP\_load\_store()** is similar to **X509\_LOOKUP\_load\_store\_ex()** but uses NULL for the library context *libctx* and property query *propq*.

**X509\_LOOKUP\_load\_file\_ex()**, **X509\_LOOKUP\_load\_file()**, **X509\_LOOKUP\_add\_dir()**, **X509\_LOOKUP\_add\_store\_ex()**, **X509\_LOOKUP\_add\_store()**, **X509\_LOOKUP\_load\_store\_ex()** and **X509\_LOOKUP\_load\_store()** are implemented as macros that use **X509\_LOOKUP\_ctrl()**.

**X509\_LOOKUP\_by\_subject\_ex()**, **X509\_LOOKUP\_by\_subject()**, **X509\_LOOKUP\_by\_issuer\_serial()**, **X509\_LOOKUP\_by\_fingerprint()**, and

**X509\_LOOKUP\_by\_alias()** look up certificates and CRLs in the **X509\_STORE(3)** associated with the **X509\_LOOKUP** using different criteria, where the looked up object is stored in *ret*. Some of the underlying **X509\_LOOKUP\_METHOD**s will also cache objects matching the criteria in the associated **X509\_STORE**, which makes it possible to handle cases where the criteria have more than one hit.

### Control Commands

The **X509\_LOOKUP\_METHOD**s built into OpenSSL recognize the following **X509\_LOOKUP\_ctrl()** *cmds*:

#### **X509\_L\_FILE\_LOAD**

This is the command that **X509\_LOOKUP\_load\_file\_ex()** and **X509\_LOOKUP\_load\_file()** use. The filename is passed in *argc*, and the type in *argl*.

#### **X509\_L\_ADD\_DIR**

This is the command that **X509\_LOOKUP\_add\_dir()** uses. The directory specification is passed in *argc*, and the type in *argl*.

#### **X509\_L\_ADD\_STORE**

This is the command that **X509\_LOOKUP\_add\_store\_ex()** and **X509\_LOOKUP\_add\_store()** use. The URI is passed in *argc*.

#### **X509\_L\_LOAD\_STORE**

This is the command that **X509\_LOOKUP\_load\_store\_ex()** and **X509\_LOOKUP\_load\_store()** use. The URI is passed in *argc*.

### RETURN VALUES

**X509\_LOOKUP\_new()** returns a **X509\_LOOKUP** pointer when successful, or NULL on error.

**X509\_LOOKUP\_init()** and **X509\_LOOKUP\_shutdown()** return 1 on success, or 0 on error.

**X509\_LOOKUP\_ctrl()** returns -1 if the **X509\_LOOKUP** doesn't have an associated **X509\_LOOKUP\_METHOD**, or 1 if the doesn't have a control function. Otherwise, it returns what the control function in the **X509\_LOOKUP\_METHOD** returns, which is usually 1 on success and 0 in error.

**X509\_LOOKUP\_get\_store()** returns a **X509\_STORE** pointer if there is one, otherwise NULL.

**X509\_LOOKUP\_by\_subject\_ex()**, **X509\_LOOKUP\_by\_subject()**, **X509\_LOOKUP\_by\_issuer\_serial()**, **X509\_LOOKUP\_by\_fingerprint()**, and **X509\_LOOKUP\_by\_alias()** all return 0 if there is no **X509\_LOOKUP\_METHOD** or that method

doesn't implement the corresponding function. Otherwise, it returns what the corresponding function in the **X509\_LOOKUP\_METHOD** returns, which is usually 1 on success and 0 in error.

#### SEE ALSO

**X509\_LOOKUP\_METHOD(3)**, **X509\_STORE(3)**

#### HISTORY

The functions **X509\_LOOKUP\_by\_subject\_ex()** and **X509\_LOOKUP\_ctrl\_ex()** were added in OpenSSL 3.0.

The macros **X509\_LOOKUP\_load\_file\_ex()**, **X509\_LOOKUP\_load\_store\_ex()** and **X509\_LOOKUP\_add\_store\_ex()** were added in OpenSSL 3.0.

#### COPYRIGHT

Copyright 2020-2021 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>.