

# globus gsi proxy ssl Reference Manual

## 1.5

Generated by Doxygen 1.2.18

Fri Jun 26 15:22:24 2009

## Contents

<a href="#">1</a>	<a href="#">Globus GSI Proxy SSL API</a>	<a href="#">1</a>
<a href="#">2</a>	<a href="#">globus gsi proxy ssl Module Index</a>	<a href="#">1</a>
<a href="#">3</a>	<a href="#">globus gsi proxy ssl Data Structure Index</a>	<a href="#">1</a>
<a href="#">4</a>	<a href="#">globus gsi proxy ssl Module Documentation</a>	<a href="#">2</a>
<a href="#">5</a>	<a href="#">globus gsi proxy ssl Data Structure Documentation</a>	<a href="#">11</a>

## 1 Globus GSI Proxy SSL API

The `globusgsi.proxy.ssl` library provides the ability to create a `PROXYCERTINFO` extension for inclusion in an X509 certificate. The current specification for the extension is described in the Internet Draft Document: `draft-ietf-pkix-proxy-08.txt`

The library conforms to the ASN1 implementation in the `OPENSSL` library (0.9.6, formerly `SSLeay`), and provides an interface to convert from a DER encoded `PROXYCERTINFO` to its internal structure and vice-versa.

## 2 globus gsi proxy ssl Module Index

### 2.1 globus gsi proxy ssl Modules

Here is a list of all modules:

<a href="#">ProxyCertInfo</a>	<a href="#">2</a>
<a href="#">ProxyPolicy</a>	<a href="#">7</a>

## 3 globus gsi proxy ssl Data Structure Index

### 3.1 globus gsi proxy ssl Data Structures

Here are the data structures with brief descriptions:

<a href="#">PROXYCERTINFO_st</a>	<a href="#">11</a>
<a href="#">PROXYPOLICY_st</a>	<a href="#">11</a>

## 4 globus gsi proxy ssl Module Documentation

### 4.1 ProxyCertInfo

#### Data Structures

struct [PROXYCERTINFO](#)st

#### ASN1\_METHOD

ASN1\_METHOD [PROXYCERTINFOasn1meth\(\)](#)

#### New

PROXYCERTINFO [PROXYCERTINFOnew\(\)](#)

#### Free.

void [PROXYCERTINFOfree](#)(PROXYCERTINFO certinfo)

#### Duplicate

PROXYCERTINFO [PROXYCERTINFOdup](#)(PROXYCERTINFO certinfo)

#### Compare

int [PROXYCERTINFOcmp](#)(const PROXYCERTINFO a, const PROXYCERTINFO b)

#### Print to a BIO stream

int [PROXYCERTINFOprint](#)(BIO bp, PROXYCERTINFO certinfo)

#### Print To Stream

int [PROXYCERTINFOprint\\_fp](#)(FILE fp, PROXYCERTINFO certinfo)

#### Set the Policy Field

int [PROXYCERTINFOsetpolicy](#)(PROXYCERTINFO certinfo, PROXYPOLICY policy)

#### Get the Policy Field

PROXYPOLICY [PROXYCERTINFOgetpolicy](#)(PROXYCERTINFO certinfo)

#### Set the Path Length Field

int [PROXYCERTINFOsetpathlength](#)(PROXYCERTINFO certinfo, long pathlength)

## Get Path Length Field

```
long PROXYCERTINFOgetpath.length(PROXYCERTINFO cert.info)
```

## Convert PROXYCERTINFO to DER encoded form

```
int i2d.PROXYCERTINFO(PROXYCERTINFO cert.info, unsigned char pp)
```

## Convert a PROXYCERTINFO to internal form

```
PROXYCERTINFO d2i.PROXYCERTINFO(PROXYCERTINFO cert.info, unsigned char pp, long length)
```

## Convert old PROXYCERTINFO to DER encoded form

```
int i2d.PROXYCERTINFOOLD (PROXYCERTINFO cert.info, unsigned char pp)
```

## Convert a old PROXYCERTINFO to internal form

```
PROXYCERTINFO d2i.PROXYCERTINFOOLD (PROXYCERTINFO cert.info, unsigned char pp, long length)
```

## 4.1.1 Detailed Description

Author:

Sam Meder , Sam Lang

The proxycertinfo.h file defines a method of maintaining information about proxy certificates.

## 4.1.2 Function Documentation

## 4.1.2.1 ASN1METHOD PROXYCERTINFO .asn1.meth ()

Define the functions required for manipulating a PROXYCERTINFO and its ASN1 form.

Creates an ASN1METHOD structure, which contains pointers to routines that convert any PROXYCERTINFO structure to its associated ASN1 DER encoded form and vice-versa.

Returns:

the ASN1METHOD object

## 4.1.2.2 PROXYCERTINFO PROXYCERTINFO .new ()

Create a new PROXYCERTINFO.

Allocates and initializes a new PROXYCERTINFO structure.

Returns:

pointer to the new PROXYCERTINFO

4.1.2.3 void PROXYCERTINFO\_free (PROXYCERTINFO cert.info)

Free a PROXYCERTINFO.

Parameters:

cert.info pointer to the PROXYCERTINFO structure to be freed.

4.1.2.4 PROXYCERTINFO PROXYCERTINFO\_dup (PROXYCERTINFO cert.info)

Makes a copy of a PROXYCERTINFO.

Makes a copy of a PROXYCERTINFO structure

Parameters:

cert.info the PROXYCERTINFO structure to copy

Returns:

the copied PROXYCERTINFO structure

4.1.2.5 int PROXYCERTINFO\_cmp (const PROXYCERTINFO a, const PROXYCERTINFO b)

Compares two PROXYCERTINFO structures

Parameters:

a pointer to the first PROXYCERTINFO structure

b pointer to the second PROXYCERTINFO structure

Returns:

an integer - the result of the comparison. The comparison compares each of the fields, so if any of those fields are not equal then a nonzero value is returned. Equality is indicated by returning a 0.

4.1.2.6 int PROXYCERTINFO\_print (BIO bp, PROXYCERTINFO cert.info)

print the PROXYCERTINFO structure to stdout

Parameters:

bp the BIO to print to

cert.info the PROXYCERTINFO to print

Returns:

1 on success, 0 on error

4.1.2.7 int PROXYCERTINFO\_print\_fp (FILE fp, PROXYCERTINFO cert.info)

print the PROXYCERTINFO structure to the specified stream

Parameters:

fp the file stream (FILE \*) to print to

cert.info the PROXYCERTINFO structure to print

Returns:

the number of characters printed

#### 4.1.2.8 int PROXYCERTINFO\_set\_policy (PROXYCERTINFO cert\_info, PROXYPOLICY policy)

Sets the policy on the PROXYCERTINFO. Since this is an optional field in the ASN1 encoding, this variable can be set to NULL through this function - which means that when the PROXYCERTINFO is encoded the policy won't be included.

Parameters:

cert\_info the PROXYCERTINFO object to set the policy of  
policy the PROXYPOLICY to set it to

Returns:

1 if success, 0 if error

#### 4.1.2.9 PROXYPOLICY PROXYCERTINFO\_get\_policy (PROXYCERTINFO cert\_info)

Gets the policy on the PROXYCERTINFO

Parameters:

cert\_info the PROXYCERTINFO to get the policy of

Returns:

the PROXYPOLICY of the PROXYCERTINFO

#### 4.1.2.10 int PROXYCERTINFO\_set\_path\_length (PROXYCERTINFO cert\_info, long path\_length)

Sets the path length of the PROXYCERTINFO. The path length specifies the maximum depth of the path of the Proxy Certificates that can be signed by an End Entity Certificate (EEC) or Proxy Certificate.

Since this is an optional field in its ASN1 coded representation, it can be set to NULL through this function - which means that it won't be included in the encoding.

Parameters:

cert\_info the PROXYCERTINFO to set the path length of  
path\_length the path length to set it to if -1 is passed in, the path length gets unset, which configures the PROXYCERTINFO to not include the path length in the DER encoding

Returns:

1 on success, 0 on error

#### 4.1.2.11 long PROXYCERTINFO\_get\_path\_length (PROXYCERTINFO cert\_info)

Gets the path length of the PROXYCERTINFO.

See also:

[PROXYCERTINFO\\_set\\_path\\_length](#)

Parameters:

cert\_info the PROXYCERTINFO to get the path length from

Returns:

the path length of the PROXYCERTINFO, or -1 if not set

4.1.2.12 int i2dPROXYCERTINFO (PROXYCERTINFO certInfo, unsigned char pp)

Converts the PROXYCERTINFO structure from internal format to a DER encoded ASN.1 string

Parameters:

certInfo the PROXYCERTINFO structure to convert  
pp the resulting DER encoded string

Returns:

the length of the DER encoded string

4.1.2.13 PROXYCERTINFO d2i\_PROXYCERTINFO (PROXYCERTINFO certInfo, unsigned char pp, long length)

Convert from a DER encoded ASN.1 string of a PROXYCERTINFO to its internal structure

Parameters:

certInfo the resulting PROXYCERTINFO in internal form  
pp the DER encoded ASN.1 string containing the PROXYCERTINFO  
length the length of the buffer

Returns:

the resulting PROXYCERTINFO in internal form

4.1.2.14 int i2dPROXYCERTINFO\_OLD (PROXYCERTINFO certInfo, unsigned char pp)

Converts the old PROXYCERTINFO structure from internal format to a DER encoded ASN.1 string

Parameters:

certInfo the old PROXYCERTINFO structure to convert  
pp the resulting DER encoded string

Returns:

the length of the DER encoded string

4.1.2.15 PROXYCERTINFO d2i\_PROXYCERTINFO\_OLD (PROXYCERTINFO certInfo, unsigned char pp, long length)

Convert from a DER encoded ASN.1 string of a old PROXYCERTINFO to its internal structure

Parameters:

certInfo the resulting old PROXYCERTINFO in internal form  
pp the DER encoded ASN.1 string containing the old PROXYCERTINFO  
length the length of the buffer

Returns:

the resulting old PROXYCERTINFO in internal form

## 4.2 ProxyPolicy

### Data Structures

struct [PROXYPOLICY\\_st](#)

### Get a method for ASN1 conversion

ASN1\_METHOD [PROXYPOLICY\\_asn1meth\(\)](#)

### New

PROXYPOLICY [PROXYPOLICY\\_new\(\)](#)

### Free

void [PROXYPOLICY\\_free](#)(PROXYPOLICY policy)

### Duplicate

PROXYPOLICY [PROXYPOLICY\\_dup](#)(PROXYPOLICY policy)

### Compare

int [PROXYPOLICY\\_cmp](#)(const PROXYPOLICY a, const PROXYPOLICY b)

### Print to a BIO stream

int [PROXYPOLICY\\_print](#)(BIO bp, PROXYPOLICY policy)

### Print to a File Stream

int [PROXYPOLICY\\_print\\_fp](#)(FILE fp, PROXYPOLICY policy)

### Set the Policy Language Field

int [PROXYPOLICY\\_set\\_policy\\_language](#)(PROXYPOLICY policy, ASN1\_OBJECT policy\_language)

### Get the Policy Language Field

ASN1\_OBJECT [PROXYPOLICY\\_get\\_policy\\_language](#)(PROXYPOLICY policy)

### Set the Policy Field

int [PROXYPOLICY\\_set\\_policy](#)(PROXYPOLICY proxypolicy, unsigned char policy, int length)



### Get the Policy Field

unsigned char [PROXYPOLICY\\_get\\_policy](#) (PROXYPOLICY policy, int length)

### Convert from Internal to DER encoded form

int [i2d\\_PROXYPOLICY](#) (PROXYPOLICY a, unsigned char pp)

### Convert from DER encoded form to Internal

PROXYPOLICY [d2i\\_PROXYPOLICY](#) (PROXYPOLICY a, unsigned char pp, long length)

#### 4.2.1 Detailed Description

##### Author:

Sam Meder , Sam Lang

The proxypolicy set of data structures and functions provides an interface to generating a PROXYPOLICY structure which is maintained as a field in the PROXYCERTINFO structure, and ultimately gets written to a DER encoded string.

##### See also:

Further Information about proxy policies is available in [the 509 Proxy Certificate Profile](#) document.

#### 4.2.2 Function Documentation

##### 4.2.2.1 ASN1METHOD PROXYPOLICY \_asn1\_meth ()

Creates an ASN1METHOD structure, which contains pointers to routines that convert any PROXYPOLICY structure to its associated ASN1 DER encoded form and vice-versa.

##### Returns:

the ASN1METHOD object

##### 4.2.2.2 PROXYPOLICY PROXYPOLICY \_new ()

Allocates and initializes a new PROXYPOLICY structure.

##### Returns:

pointer to the new PROXYPOLICY

##### 4.2.2.3 void PROXYPOLICY\_free (PROXYPOLICY policy)

Frees a PROXYPOLICY

##### Parameters:

policy the proxy policy to free

#### 4.2.2.4 PROXYPOLICY PROXYPOLICY \_dup (PROXYPOLICY policy)

Makes a copy of the proxypolicy - this function allocates space for a new PROXYPOLICY, so the returned PROXYPOLICY must be freed when its no longer needed

Parameters:

policy the proxy policy to copy

Returns:

the new PROXYPOLICY

#### 4.2.2.5 int PROXYPOLICY \_cmp (const PROXYPOLICY a, const PROXYPOLICY b)

Compares two PROXYPOLICY structs for equality This function rst compares the policy language numeric id's, if they're equal, it then compares the two policies.

Returns:

0 if equal, nonzero if not

#### 4.2.2.6 int PROXYPOLICY \_print (BIO bp, PROXYPOLICY policy)

Prints the PROXYPOLICY struct using the BIO stream

Parameters:

bp the BIO stream to print to

policy the PROXYPOLICY to print

Returns:

1 on success, 0 on error

#### 4.2.2.7 int PROXYPOLICY \_print \_fp (FILE fp, PROXYPOLICY policy)

Prints the PROXYPOLICY to the le stream FILE

Parameters:

fp the FILE stream to print to

policy the PROXYPOLICY to print

Returns:

number of bytes printed, -2 or -1 on error

#### 4.2.2.8 int PROXYPOLICY \_set.policy\_language (PROXYPOLICY policy, ASN1\_OBJECT policy\_language)

Sets the policy language of the PROXYPOLICY

Parameters:

policy the PROXYPOLICY to set the policy language of

policy\_language the policy language to set it to

Returns:

1 on success, 0 on error

#### 4.2.2.9 ASN1OBJECT PROXYPOLICY \_get.policy.language (PROXYPOLICY policy)

Gets the policy language of the PROXYPOLICY

Parameters:

policy the proxy policy to get the policy language of

Returns:

the policy language as an ASN1OBJECT

#### 4.2.2.10 int PROXYPOLICY \_set.policy (PROXYPOLICY proxypolicy, unsigned char policy, int length)

Sets the policy of the PROXYPOLICY

Parameters:

proxypolicy the proxy policy to set the policy of

policy the policy to set it to

length the length of the policy

Returns:

1 on success, 0 on error

#### 4.2.2.11 unsigned char PROXYPOLICY \_get.policy (PROXYPOLICY policy, int length)

Gets the policy of a PROXYPOLICY

Parameters:

policy the PROXYPOLICY to get the policy of

length the length of the returned policy - this value gets set by this function

Returns:

the policy

#### 4.2.2.12 int i2dPROXYPOLICY (PROXYPOLICY a, unsigned char pp)

Converts a PROXYPOLICY from its internal structure to a DER encoded form

Parameters:

a the PROXYPOLICY to convert

pp the buffer to put the DER encoding in

Returns:

the length of the DER encoding in bytes

#### 4.2.2.13 PROXYPOLICY\_d2i\_PROXYPOLICY (PROXYPOLICY a, unsigned char pp, long length)

Converts the PROXYPOLICY from its DER encoded form to an internal PROXYPOLICY structure

Parameters:

- a the PROXYPOLICY struct to set
- pp the DER encoding to get the PROXYPOLICY from
- length the length of the DER encoding

Returns:

the resulting PROXYPOLICY in its internal structure form - this variable has been allocated using routines, so it needs to be freed once its no longer used

## 5 globus gsi proxy ssl Data Structure Documentation

### 5.1 PROXYCERTINFO\_st Struct Reference

#### 5.1.1 Detailed Description

This typedef maintains information about a proxy certificate.

Note:

NOTE: The API provides functions to manipulate the fields of a PROXYCERTINFO. Accessing the fields directly is not a good idea.

Parameters:

- path\_length an optional field in the ANS.1 DER encoding, it specifies the maximum depth of the path of Proxy Certificates that can be signed by this End Entity Certificate or Proxy Certificate.
- policy a non-optional field in the ANS.1 DER encoding, specifies policies on the use of this certificate.

### 5.2 PROXYPOLICY\_st Struct Reference

#### 5.2.1 Detailed Description

Note:

NOTE: The API provides functions to manipulate the fields of a PROXYPOLICY. Accessing the fields directly will not work.

This typedef maintains information about the policies that have been placed on a proxy certificate

Parameters:

- policy\_language defines which policy language is to be used to define the policies
- policy the policy that determines the policies on a certificate

---

## Index

d2i\_PROXYCERTINFO  
    proxycertinfo, 6  
d2i\_PROXYCERTINFO\_OLD  
    proxycertinfo, 6  
d2i\_PROXYPOLICY  
    proxypolicy, 10  
  
i2d\_PROXYCERTINFO  
    proxycertinfo, 5  
i2d\_PROXYCERTINFO\_OLD  
    proxycertinfo, 6  
i2d\_PROXYPOLICY  
    proxypolicy, 10  
  
ProxyCertInfo, 2  
proxycertinfo  
    d2i\_PROXYCERTINFO, 6  
    d2i\_PROXYCERTINFO\_OLD, 6  
    i2d\_PROXYCERTINFO, 5  
    i2d\_PROXYCERTINFO\_OLD, 6  
    PROXYCERTINFOasn1meth, 3  
    PROXYCERTINFOcmp, 4  
    PROXYCERTINFOdup, 4  
    PROXYCERTINFOfree, 3  
    PROXYCERTINFOgetpathlength, 5  
    PROXYCERTINFOgetpolicy, 5  
    PROXYCERTINFOnew, 3  
    PROXYCERTINFOprint, 4  
    PROXYCERTINFOprint\_fp, 4  
    PROXYCERTINFOsetpathlength, 5  
    PROXYCERTINFOsetpolicy, 4  
PROXYCERTINFOasn1meth  
    proxycertinfo, 3  
PROXYCERTINFOcmp  
    proxycertinfo, 4  
PROXYCERTINFOdup  
    proxycertinfo, 4  
PROXYCERTINFOfree  
    proxycertinfo, 3  
PROXYCERTINFOgetpathlength  
    proxycertinfo, 5  
PROXYCERTINFOgetpolicy  
    proxycertinfo, 5  
PROXYCERTINFOnew  
    proxycertinfo, 3  
PROXYCERTINFOprint  
    proxycertinfo, 4  
PROXYCERTINFOprint\_fp  
    proxycertinfo, 4  
PROXYCERTINFOsetpathlength  
    proxycertinfo, 5  
PROXYCERTINFOsetpolicy  
    proxycertinfo, 4  
PROXYCERTINFOst, 11  
ProxyPolicy, 7  
proxypolicy  
    d2i\_PROXYPOLICY, 10  
    i2d\_PROXYPOLICY, 10  
    PROXYPOLICYasn1meth, 8  
    PROXYPOLICYcmp, 9  
    PROXYPOLICYdup, 8  
    PROXYPOLICYfree, 8  
    PROXYPOLICYgetpolicy, 10  
    PROXYPOLICYgetpolicy\_language, 9  
    PROXYPOLICYnew, 8  
    PROXYPOLICYprint, 9  
    PROXYPOLICYprint\_fp, 9  
    PROXYPOLICYsetpolicy, 10  
    PROXYPOLICYsetpolicy\_language, 9  
PROXYPOLICYasn1meth  
    proxypolicy, 8  
PROXYPOLICYcmp  
    proxypolicy, 9  
PROXYPOLICYdup  
    proxypolicy, 8  
PROXYPOLICYfree  
    proxypolicy, 8  
PROXYPOLICYgetpolicy  
    proxypolicy, 10  
PROXYPOLICYgetpolicy\_language  
    proxypolicy, 9  
PROXYPOLICYnew  
    proxypolicy, 8  
PROXYPOLICYprint  
    proxypolicy, 9  
PROXYPOLICYprint\_fp  
    proxypolicy, 9  
PROXYPOLICYsetpolicy  
    proxypolicy, 10  
PROXYPOLICYsetpolicy\_language  
    proxypolicy, 9  
PROXYPOLICYst, 11

---