globus gsi proxy ssl Reference Manual

1.5

Generated by Doxygen 1.2.18

Tue Aug 11 22:20:49 2009

Contents

1 Globus GSI Proxy SSL API

The globusgsi_proxy_ssl library provides the ability to create a PROXYCERTINFO extension for inclusion in an X509 certi cate. The current speci cation 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:

3 globus gsi proxy ssl Data Structure Index

3.1 globus gsi proxy ssl Data Structures

Here are the data structures with brief descriptions:

4 globus gsi proxy ssl Module Documentation

4.1 ProxyCertInfo

Data Structures

struct PROXYCERTINFO_st

ASN1_METHOD

ASN1_METHOD PROXYCERTINFO_asn1meth()

New

PROXYCERTINFO PROXYCERTINFO_new()

Free.

void PROXYCERTINFO_free(PROXYCERTINFO cert_info)

Duplicate

PROXYCERTINFO PROXYCERTINFO_dup(PROXYCERTINFO cert_info)

Compare

int PROXYCERTINFO_cmp(const PROXYCERTINFO a, const PROXYCERTINFO b)

Print to a BIO stream

int PROXYCERTINFO_print(BIO bp, PROXYCERTINFO cert_info)

Print To Stream

int PROXYCERTINFO_print_fp(FILE fp, PROXYCERTINFO cert_info)

Set the Policy Field

int PROXYCERTINFO_set_policy(PROXYCERTINFO cert_info, PROXYPOLICY policy)

Get the Policy Field

PROXYPOLICY PROXYCERTINFO_get_policy(PROXYCERTINFO cert_info)

Set the Path Length Field

int PROXYCERTINFO_set_path_length(PROXYCERTINFO cert_info, long path_length)

Get Path Length Field

long PROXYCERTINFO_get_path_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_PROXYCERTINFO_OLD (PROXYCERTINFO cert_info, unsigned char pp)

Convert a old PROXYCERTINFO to internal form

PROXYCERTINFO d2i_PROXYCERTINFO_OLD (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 ASN1_METHOD PROXYCERTINFO_asn1_meth ()

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

Creates an ASN1_METHOD structure, which contains pointers to routines that convert any PROXYCERTINFO structure to its associated ASN1 DER encoded form and vice-versa.

Returns:
the ASN1_METHOD 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 rst PROXYCERTINFO structure
b pointer to the second PROXYCERTINFO structure

Returns:
an integer - the result of the comparison. The comparison compares each of the elds, so if any of those elds 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 speci ed le stream

Parameters:
fp the le 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 i2d_PROXYCERTINFO (PROXYCERTINFO cert_info, unsigned char pp)

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

Parameters:
cert_info 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 cert_info, unsigned char pp, long length)

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

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

Returns:
the resultingin PROXYCERTINFO in internal form

4.1.2.14 int i2d_PROXYCERTINFO_OLD (PROXYCERTINFO cert_info, unsigned char pp)

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

Parameters:
cert_info 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 cert_info, unsigned char pp, long length)

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

Parameters:
cert_info 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 RFC 3820 Proxy Certificate Profile document.

4.2.2 Function Documentation

4.2.2.1 ASN1_METHOD PROXYPOLICY_asn1_meth ()

Creates an ASN1_METHOD structure, which contains pointers to routines that convert any PROXYPOLICY structure to its associated ASN1 DER encoded form and vice-versa.

Returns:
the ASN1_METHOD 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 first 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 file 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 ASN1_OBJECT 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 ASN1_OBJECT

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 i2d_PROXYPOLICY (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