NAME

gnutls_pkcs12_simple_parse - API function

SYNOPSIS

#include <gnutls/pkcs12.h>

int gnutls_pkcs12_simple_parse(gnutls_pkcs12_t *p12***, const char *** *password***, gnutls_x509_privkey_t *** *key***, gnutls_x509_crt_t **** *chain***, unsigned int *** *chain_len***, gnutls_x509_crt_t **** *extra_certs***, unsigned int *** *extra_certs_len***, gnutls_x509_crl_t *** *crl***, unsigned int** *flags***);**

ARGUMENTS

gnutls_pkcs12_t p12
: A pkcs12 type

const char * password
: optional password used to decrypt the structure, bags and keys.

gnutls_x509_privkey_t * key
: a structure to store the parsed private key.

gnutls_x509_crt_t ** chain
: the corresponding to key certificate chain (may be **NULL**)

unsigned int * chain_len
: will be updated with the number of additional (may be **NULL**)

gnutls_x509_crt_t ** extra_certs
: optional pointer to receive an array of additional certificates found in the PKCS12 structure (may be **NULL**).

unsigned int * extra_certs_len
: will be updated with the number of additional certs (may be **NULL**).

gnutls_x509_crl_t * crl
: an optional structure to store the parsed CRL (may be **NULL**).

unsigned int flags
: should be zero or one of GNUTLS_PKCS12_SP_*

DESCRIPTION

This function parses a PKCS12 structure in *pkcs12* and extracts the private key, the corresponding certificate chain, any additional certificates and a CRL. The structures in *key* , *chain* *crl* , and *extra_certs* must not be initialized.

The *extra_certs* and *extra_certs_len* parameters are optional and both may be set to **NULL**. If either is non-**NULL**, then both must be set. The value for *extra_certs* is allocated using **gnutls_malloc()**.

Encrypted PKCS12 bags and PKCS8 private keys are supported, but only with password based security and the same password for all operations.

Note that a PKCS12 structure may contain many keys and/or certificates, and there is no way to identify which key/certificate pair you want. For this reason this function is useful for PKCS12 files that contain only one key/certificate pair and/or one CRL.

If the provided structure has encrypted fields but no password is provided then this function returns **GNUTLS_E_DECRYPTION_FAILED**.

Note that normally the chain constructed does not include self signed certificates, to comply with TLS' requirements. If, however, the flag **GNUTLS_PKCS12_SP_INCLUDE_SELF_SIGNED** is specified then self signed certificates will be included in the chain.

Prior to using this function the PKCS **12** structure integrity must be verified using **gnutls_pkcs12_verify_mac()**.

RETURNS

On success, **GNUTLS_E_SUCCESS** (0) is returned, otherwise a negative error value.

SINCE

3.1.0

REPORTING BUGS

Report bugs to <bugs@gnutls.org>.
Home page: https://www.gnutls.org

COPYRIGHT

SEE ALSO

The full documentation for **gnutls** is maintained as a Texinfo manual. If the /usr/local/share/doc/gnutls/ directory does not contain the HTML form visit

https://www.gnutls.org/manual/