NAME

gnutls_priority_init2 - API function

SYNOPSIS

#include <gnutls/gnutls.h>

int gnutls_priority_init2(gnutls_priority_t * *priority_cache***, const char *** *priorities***, const char **** *err_pos***, unsigned** *flags***);**

ARGUMENTS

gnutls_priority_t * priority_cache

is a **gnutls_priority_t** type.

const char * priorities

is a string describing priorities (may be **NULL**)

const char ** err_pos

In case of an error this will have the position in the string the error occurred

unsigned flags

zero or **GNUTLS_PRIORITY_INIT_DEF_APPEND**

DESCRIPTION

Sets priorities for the ciphers, key exchange methods, and macs. The *priority_cache* should be deinitialized using **gnutls_priority_deinit()**.

The **priorities** option allows you to specify a colon separated list of the cipher priorities to enable. Some keywords are defined to provide quick access to common preferences.

When *flags* is set to **GNUTLS_PRIORITY_INIT_DEF_APPEND** then the *priorities* specified will be appended to the default options.

Unless there is a special need, use the "NORMAL" keyword to apply a reasonable security level, or "NORMAL:%COMPAT" for compatibility.

"PERFORMANCE" means all the "secure" ciphersuites are enabled, limited to 128 bit ciphers and sorted by terms of speed performance.

"LEGACY" the NORMAL settings for GnuTLS 3.2.x or earlier. There is no verification profile set, and the allowed DH primes are considered weak today.

"NORMAL" means all "secure" ciphersuites. The 256-bit ciphers are included as a fallback only. The ciphers are sorted by security margin.

"PFS" means all "secure" ciphersuites that support perfect forward secrecy. The 256-bit ciphers are included as a fallback only. The ciphers are sorted by security margin.

"SECURE128" means all "secure" ciphersuites of security level 128-bit or more.

"SECURE192" means all "secure" ciphersuites of security level 192-bit or more.

"SUITEB128" means all the NSA SuiteB ciphersuites with security level of 128.

"SUITEB192" means all the NSA SuiteB ciphersuites with security level of 192.

"NONE" means nothing is enabled. This disables everything, including protocols.

"@KEYWORD1,KEYWORD2,..." The system administrator imposed settings. The provided keyword(s) will be expanded from a configuration-time provided file - default is: /usr/local/etc/gnutls/config. Any attributes that follow it, will be appended to the expanded string. If multiple keywords are provided, separated by commas, then the first keyword that exists in the configuration file will be used. At least one of the keywords must exist, or this function will return an error. Typical usage would be to specify an application specified keyword first, followed by "SYSTEM" as a default fallback. e.g., " *LIBVIRT* ,SYSTEM:!-VERS-SSL3.0" will first try to find a config file entry matching "LIBVIRT", but if that does not exist will use the entry for "SYSTEM". If "SYSTEM" does not exist either, an error will be returned. In all cases, the SSL3.0 protocol will be disabled. The system priority file entries should be formatted as "KEYWORD=VALUE", e.g., "SYSTEM=NORMAL:+ARCFOUR-128".

Special keywords are "!", "-" and "+". "!" or "-" appended with an algorithm will remove this algorithm. "+" appended with an algorithm will add this algorithm.

Check the GnuTLS manual section "Priority strings" for detailed information.

EXAMPLES

"NONE:+VERS-TLS-ALL:+MAC-ALL:+RSA:+AES-128-CBC:+SIGN-ALL:+COMP-NULL"

"NORMAL:+ARCFOUR-128" means normal ciphers plus ARCFOUR-128.

"SECURE128:-VERS-SSL3.0" means that only secure ciphers are and enabled, SSL3.0 is disabled.

"NONE:+VERS-TLS-ALL:+AES-128-CBC:+RSA:+SHA1:+COMP-NULL:+SIGN-RSA-SHA1",

"NONE:+VERS-TLS-ALL:+AES-128-CBC:+ECDHE-RSA:+SHA1:+COMP-NULL:+SIGN-RSA-SHA1:+CURVE-S

"SECURE256:+SECURE128",

Note that "NORMAL:%COMPAT" is the most compatible mode.

A **NULL** *priorities* string indicates the default priorities to be used (this is available since GnuTLS 3.3.0).

RETURNS

On syntax error **GNUTLS_E_INVALID_REQUEST** is returned, **GNUTLS_E_SUCCESS** on success, or an error code.

SINCE

3.6.3

REPORTING BUGS

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

COPYRIGHT

Copyright (C) 2001- Free Software Foundation, Inc., and others.
Copying and distribution of this file, with or without modification, are permitted in any medium without royalty provided the copyright notice and this notice are preserved.

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/