

GnuTLS



Simon Josefsson
simon@josefsson.org
<http://josefsson.org/>

Agenda

- **What is GnuTLS?**
- **What's going on? (v2.2.x)**
- **Software Patent Blues**
- **Hands-on GnuTLS:
gnutls-cli, certtool, ...**

What is GnuTLS?

What is GnuTLS?

**GnuTLS is an implementation
of the SSL/TLS standard**

– HTTP, IMAP, SMTP, POP3, ...

What is GnuTLS?

**Implements X.509/PKIX and
PKCS standards**

What is GnuTLS?

**A successful free
software project**

A successful free software project

#<name> is the package name;
#<inst> is the number of people who installed this package;
#<vote> is the number of people who use this package regularly;
#<old> is the number of people who installed, but don't use this package
regularly;
#<recent> is the number of people who upgraded this package recently;
#<no-files> is the number of people whose entry didn't contain enough
information (atime and ctime were 0).

#rank	name	inst	vote	old	recent	no-files
103	libssl0.9.8	68202	54738	2143	11317	4
112	libgnutls13	67966	53525	2809	11623	9
12165	libmatrixssl1.7	150	1	9	0	140
19482	libmatrixssl1.8	44	19	22	3	0

What is GnuTLS?

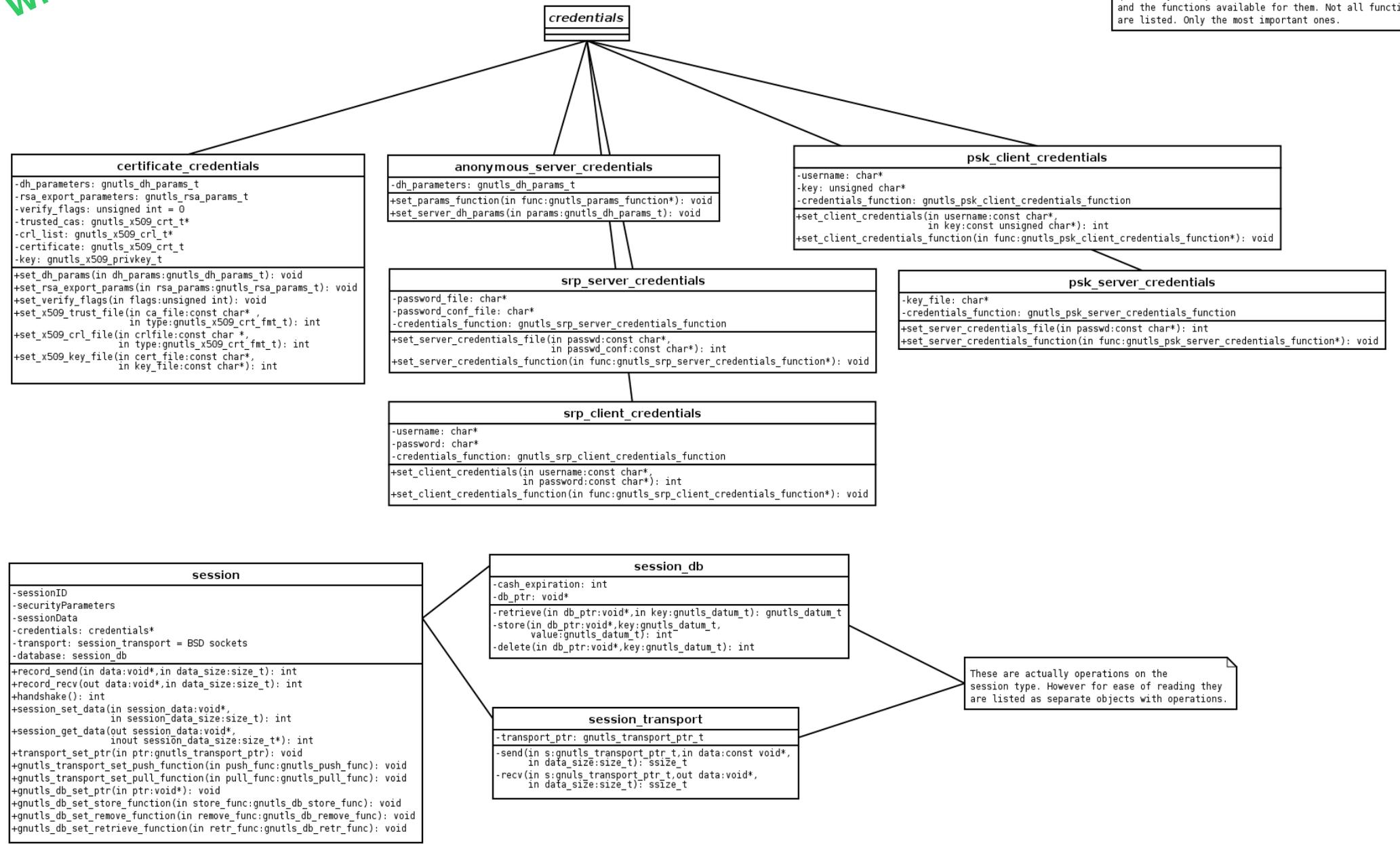
Written in C

What is GnuTLS?

Object Oriented Design

What is GnuTLS?

Since GnuTLS is implemented in C objects are not quite easy to separate. Here we list the structures and the functions available for them. Not all functions are listed. Only the most important ones.



What is GnuTLS?

Official API bindings in Guile (scheme) and C++

What is GnuTLS?

**Started early
months of 2000**

What is GnuTLS?

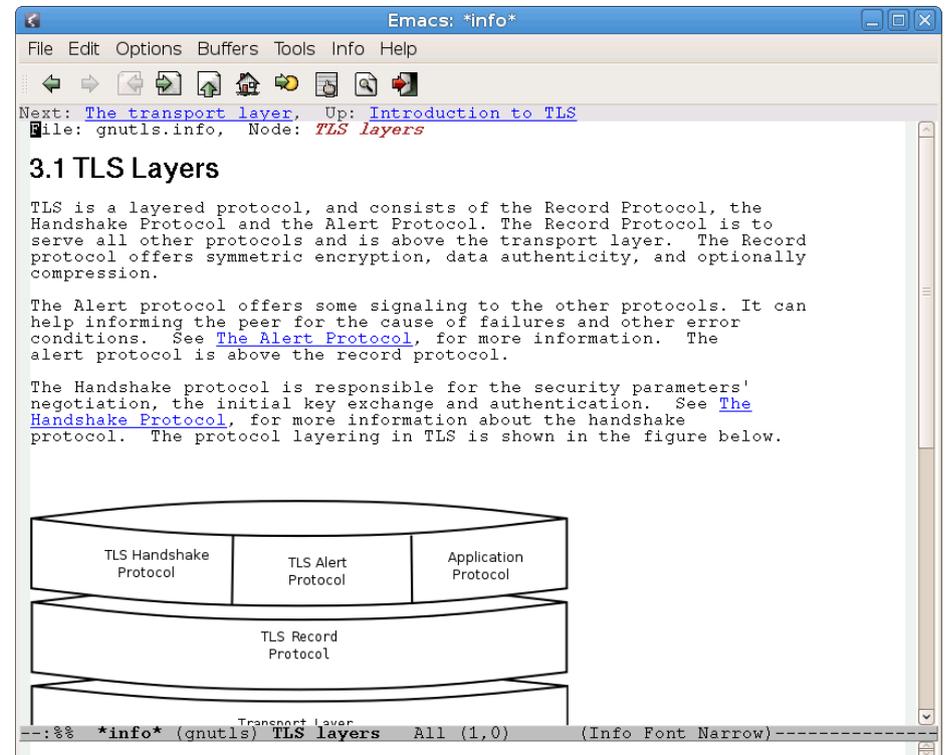
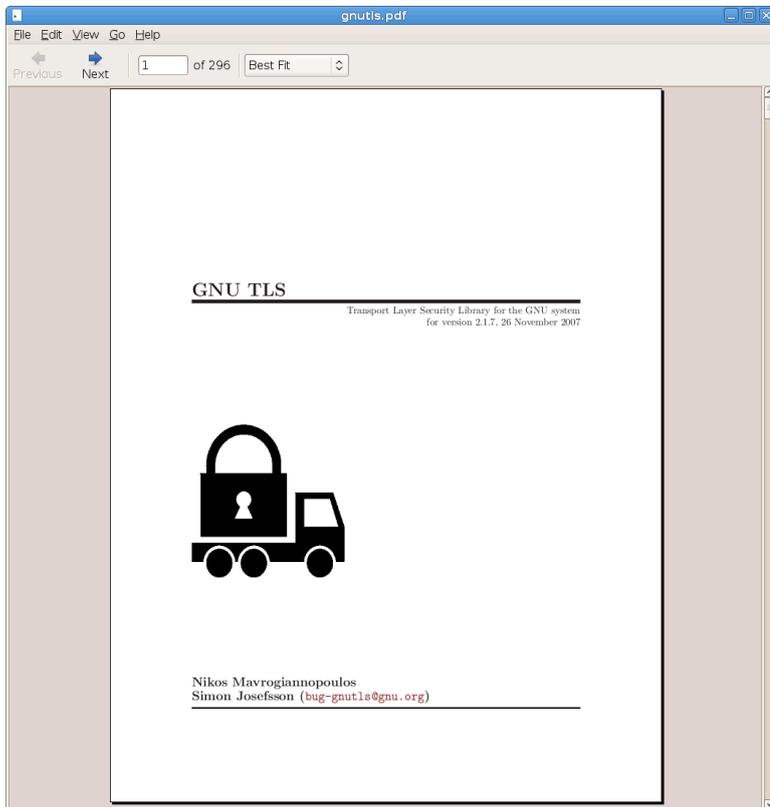
**Written by Nikos
Mavrogiannopoulos**

What is GnuTLS?

**I maintain it since
August 2004**

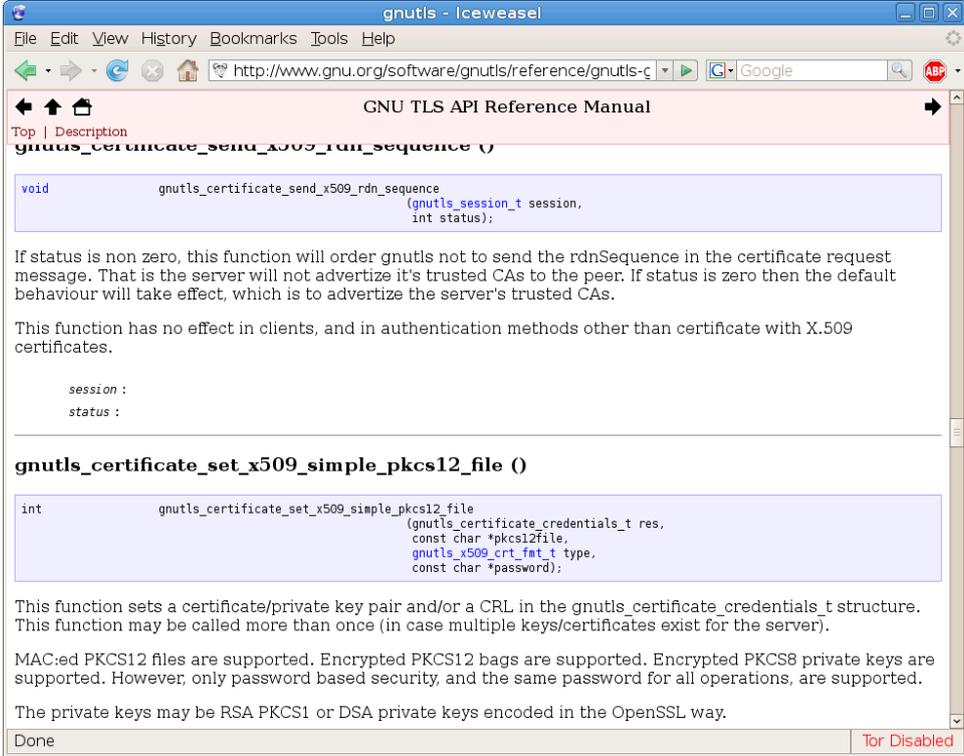
What is GnuTLS?

Reference manual



What is GnuTLS?

Documented source code



The screenshot shows a web browser window titled "gnutls - Iceweasel" displaying the GNU TLS API Reference Manual. The browser's address bar shows the URL "http://www.gnu.org/software/gnutls/reference/gnutls-c". The page title is "GNU TLS API Reference Manual". The main content area shows the function signature for `gnutls_certificate_send_x509_rdn_sequence ()` and its description. Below the function signature, there is a code block showing the function signature:

```
void gnutls_certificate_send_x509_rdn_sequence (gnutls_session_t session, int status);
```

 The description explains that if status is non zero, the function will order gnutls not to send the rdnSequence in the certificate request message. It also states that this function has no effect in clients and in authentication methods other than certificate with X.509 certificates. Below the description, there are two parameters listed: `session :` and `status :`. The next function signature is `gnutls_certificate_set_x509_simple_pkcs12_file ()`. Below it, there is a code block showing the function signature:

```
int gnutls_certificate_set_x509_simple_pkcs12_file (gnutls_certificate_credentials_t res, const char *pkcs12file, gnutls_x509_crt_fat_t type, const char *password);
```

 The description for this function states that it sets a certificate/private key pair and/or a CRL in the `gnutls_certificate_credentials_t` structure. It also mentions that MAC:ed PKCS12 files are supported, encrypted PKCS12 bags are supported, and encrypted PKCS8 private keys are supported. However, only password based security, and the same password for all operations, are supported. The private keys may be RSA PKCS1 or DSA private keys encoded in the OpenSSL way. The browser's status bar at the bottom shows "Done" and "Tor Disabled".

gnutls - Iceweasel

File Edit View History Bookmarks Tools Help

http://www.gnu.org/software/gnutls/reference/gnutls-c Google

GNU TLS API Reference Manual

Top | Description

gnutls_certificate_send_x509_rdn_sequence ()

```
void gnutls_certificate_send_x509_rdn_sequence (gnutls_session_t session, int status);
```

If status is non zero, this function will order gnutls not to send the rdnSequence in the certificate request message. That is the server will not advertize it's trusted CAs to the peer. If status is zero then the default behaviour will take effect, which is to advertize the server's trusted CAs.

This function has no effect in clients, and in authentication methods other than certificate with X.509 certificates.

session :

status :

gnutls_certificate_set_x509_simple_pkcs12_file ()

```
int gnutls_certificate_set_x509_simple_pkcs12_file (gnutls_certificate_credentials_t res, const char *pkcs12file, gnutls_x509_crt_fat_t type, const char *password);
```

This function sets a certificate/private key pair and/or a CRL in the `gnutls_certificate_credentials_t` structure. This function may be called more than once (in case multiple keys/certificates exist for the server).

MAC:ed PKCS12 files are supported. Encrypted PKCS12 bags are supported. Encrypted PKCS8 private keys are supported. However, only password based security, and the same password for all operations, are supported.

The private keys may be RSA PKCS1 or DSA private keys encoded in the OpenSSL way.

Done Tor Disabled

What is GnuTLS?

Official GNU project



What is GnuTLS?

**libtasn1,
libgcrypt,
opencdk,
libz,
liblzo**

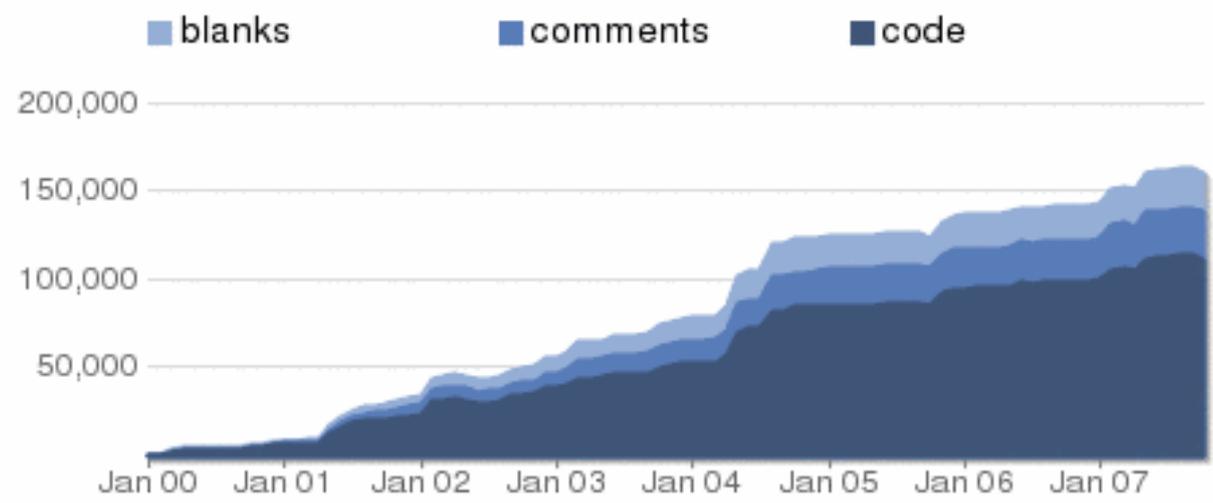
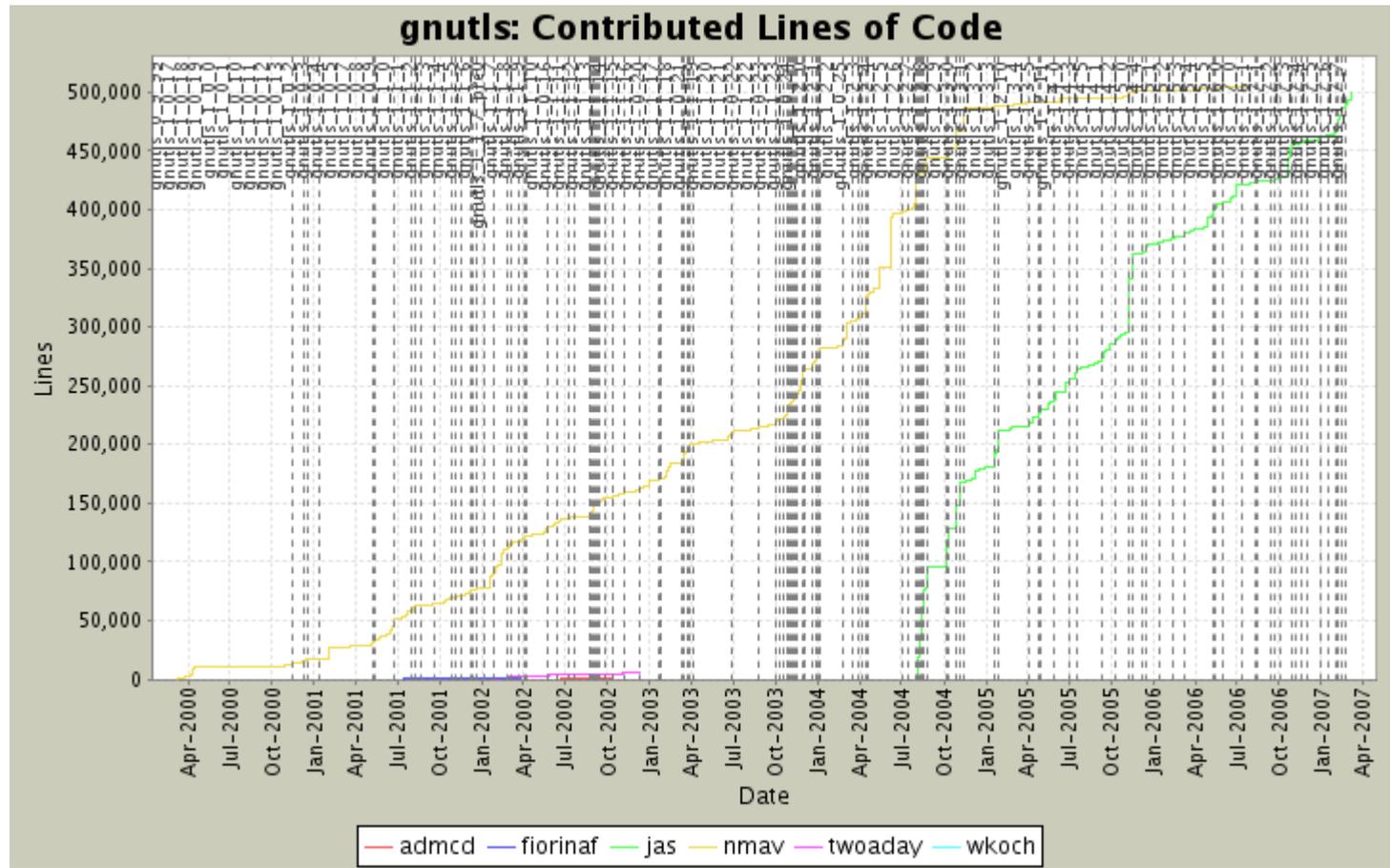
What is GnuTLS?

**Version control: Git
(before May 2007: CVS)**

What is GnuTLS?

savannah.gnu.org

What is GnuTLS?



What is GnuTLS?

September 2007: Version 2.0

What's Going On? (v2.2.x)

**What's Going On?
OpenPGP**

RFC 5081 November 2007

New!

What's Going On?
OpenPGP

**Use your OpenPGP key
during handshake**

What's Going On?
OpenPGP

Verify server OpenPGP key via web-of-trust

What's Going On?
mod_gnutls

Apache mod_gnutls work in progress

http://www.outoforder.cc/projects/apache/mod_gnutls/

What's Going On?
mod_gnutls

mod_ssl 15kLOC
mod_gnutls 3kLOC

What's Going On?
mod_gnutls

Support for Server Name Indication

What's Going On?
mod_gnutls

**Please write cool
applications!**

**(any Debian Developers
out there?)**

**What's Going On?
Secure Remote
Password**

RFC 5054 (November 2007)

New!

**What's Going On?
Secure Remote
Password**

Strong password-based authentication inside the TLS handshake

- Working mod_gnutls v.0.4.1**

TLS v1.2

- **We implemented early drafts, but the protocol has changed since then...**

What's Going On?

Opaque PRF Input

- Allows systems to provide additional randomness for master key generation**

External RSA/DSA signing

- No need to have RSA/DSA keys in same process**
- OpenPGP Scute PKCS#11 engine tested**
- Upcoming GNOME integration with SeaHorse**

What's Going On?

uClinux port

- **Embedded platforms**
- **<http://josefsson.org/uclinux/>**

Software Patent Blues

TLS Authorization Extension

Implemented in v2.0

**Patent Application
filed September 2005**

IETF Last Call in May 2006

Approved June 2006

**IETF notified about patent
in November 2006**

IETF policy on patents:

RFC 3979: Intellectual Property Rights in IETF Technology

6.1. Who Must Make an IPR Disclosure?

6.1.1. A Contributor's IPR in his or her Contribution

Any Contributor who reasonably and personally knows of IPR [...] must make a disclosure in accordance with this Section 6.

[...]

Contributors must disclose IPR meeting the description in this section; there are no exceptions to this rule.

We have removed our implementation

“This technique may be patented in the future, and it is not of crucial importance for the Internet community. After deliberation we have concluded that the best thing we can do in this situation is to encourage society not to adopt this technique. We have decided to lead the way with our own actions.”

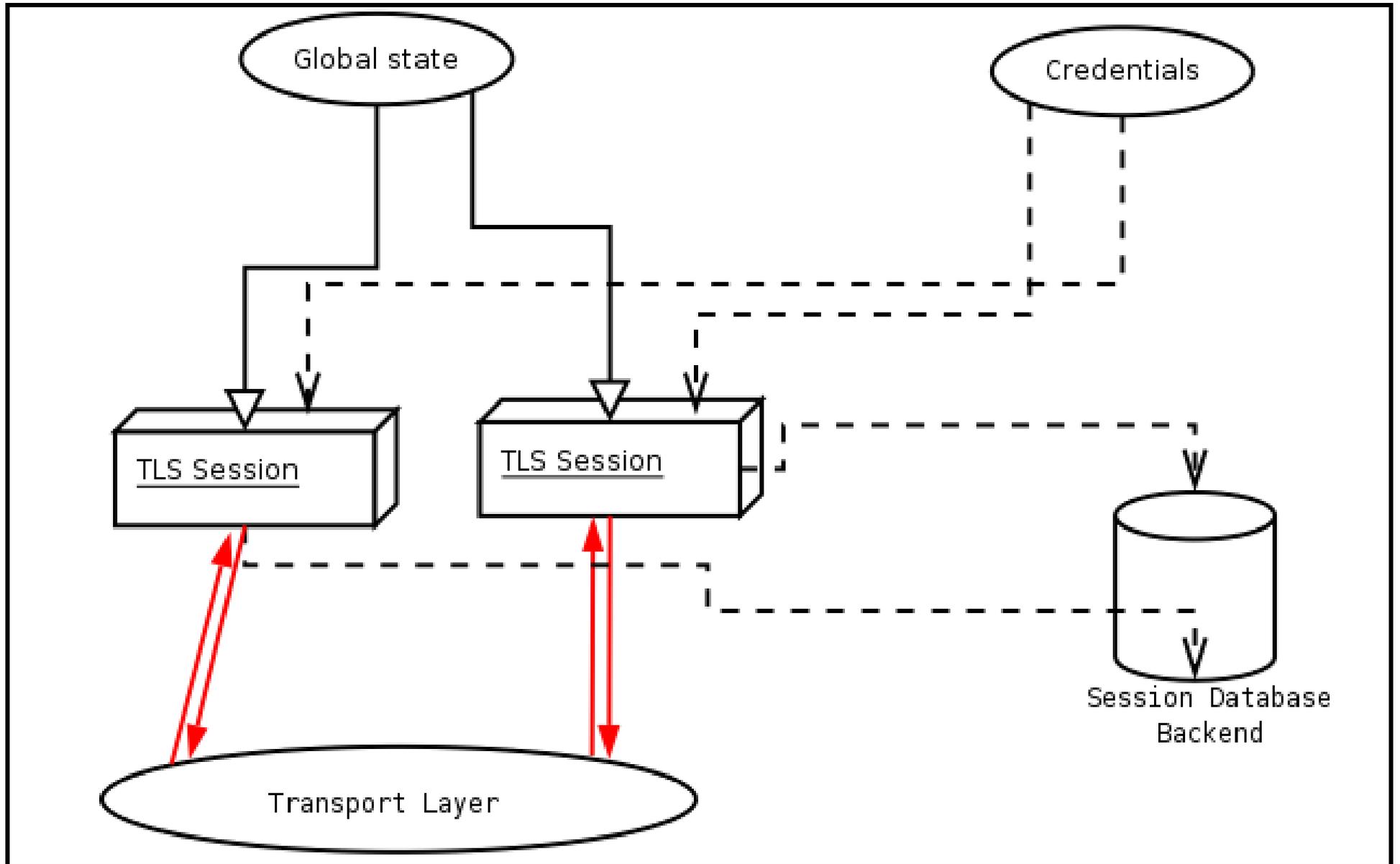
<http://www.fsf.org/news/oppose-tls-authz-standard.html>

**Please develop a
free alternative!**

Hands-on GnuTLS

- **certtool**
- **gnutls-cli**
- **gnutls-serv**

- **Generating private key**
- **Generating CA**
- **Generating server certificate**
- **Starting a test HTTPS server**
- **Generating client certificate**
- **Creating PKCS#12 blob**
- **Import into browser**
- **Connect to server**



Questions?

Answers?

Thank you for listening!

Copyright © 2007 Simon Josefsson

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.