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?

GnuTLS is an implemention of the SSL/TLS standard

- HTTP, IMAP, SMTP, POP3, ...

Implements X.509/PKIX and PKCS standards

A successful free software project

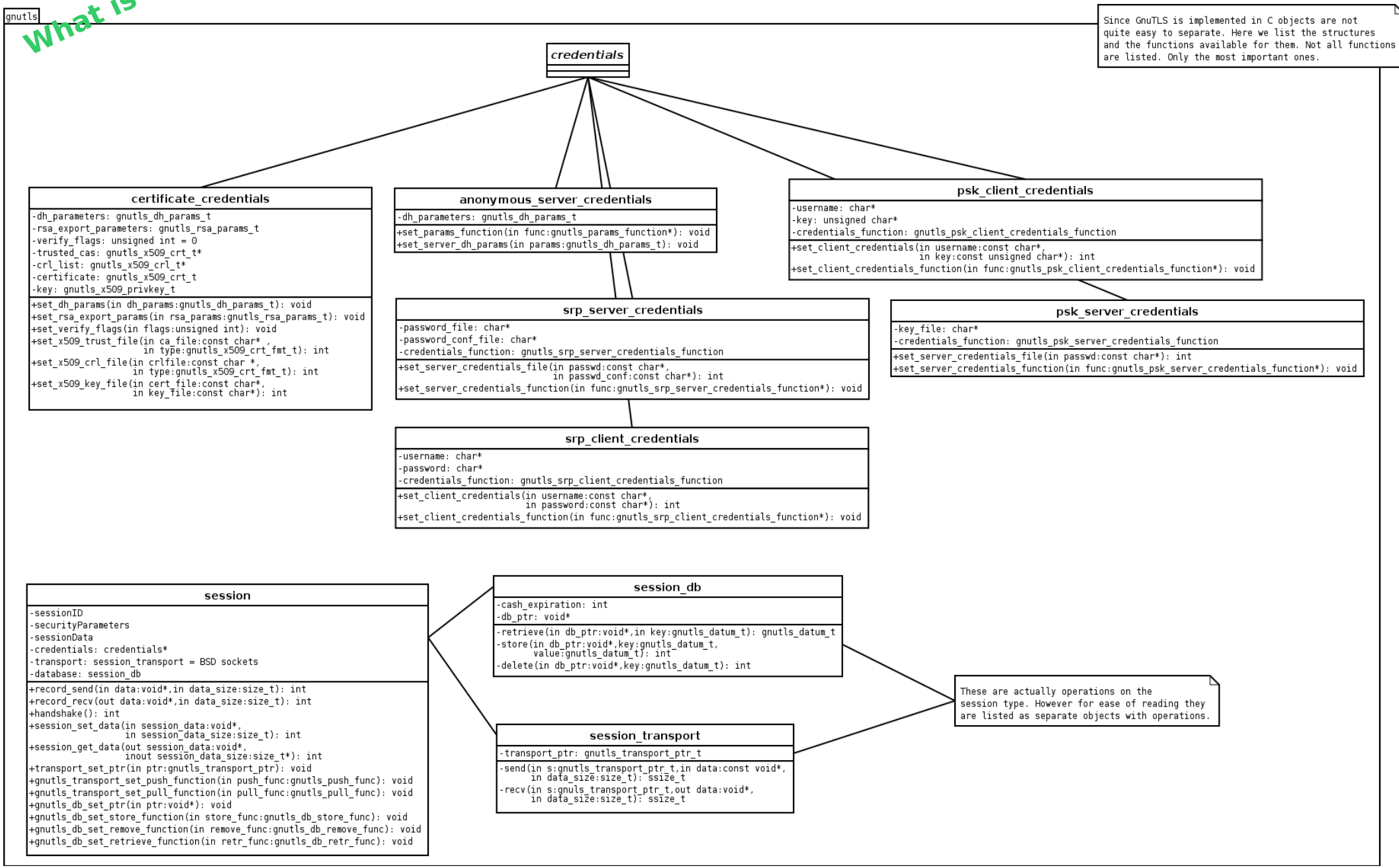
A successful free software project

```
#<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
```

Written in C

Object Oriented Design

What is GnuTLS?



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

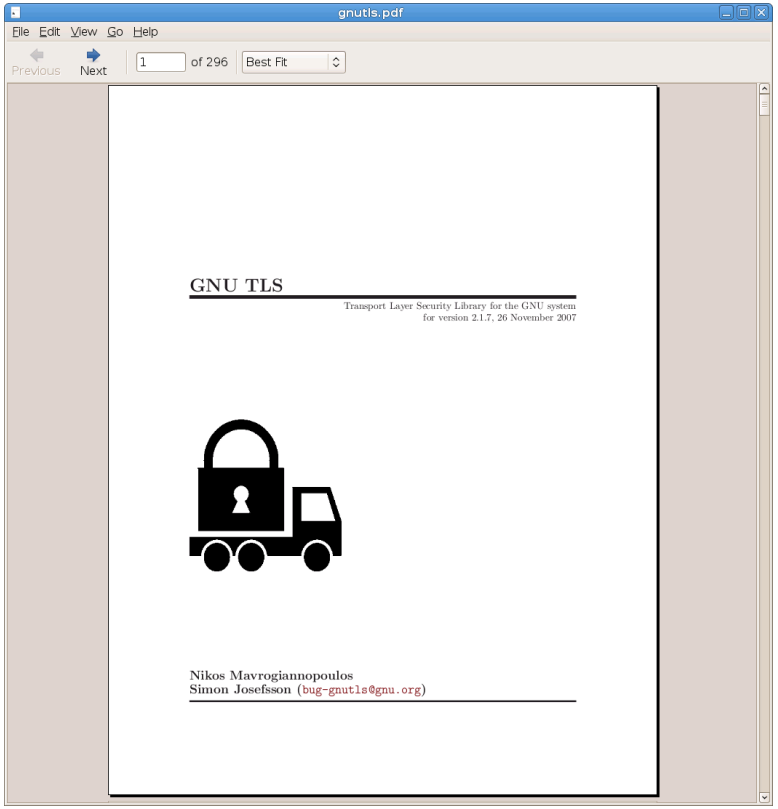
Started early months of 2000

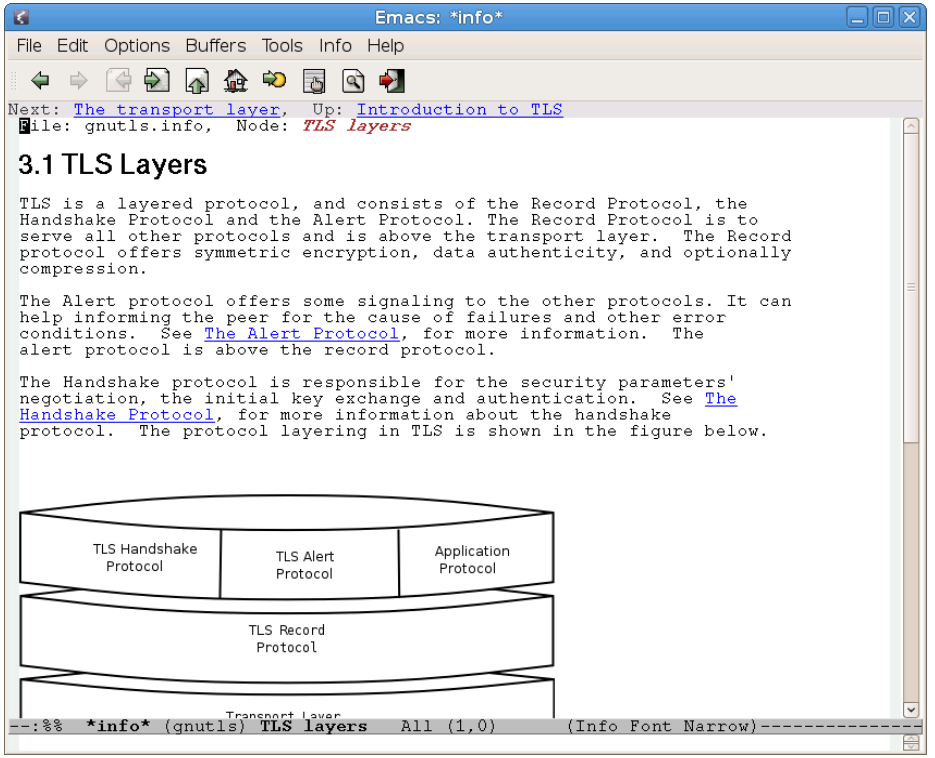
Written by Nikos Mavrogiannopoulos

I maintain it since August 2004

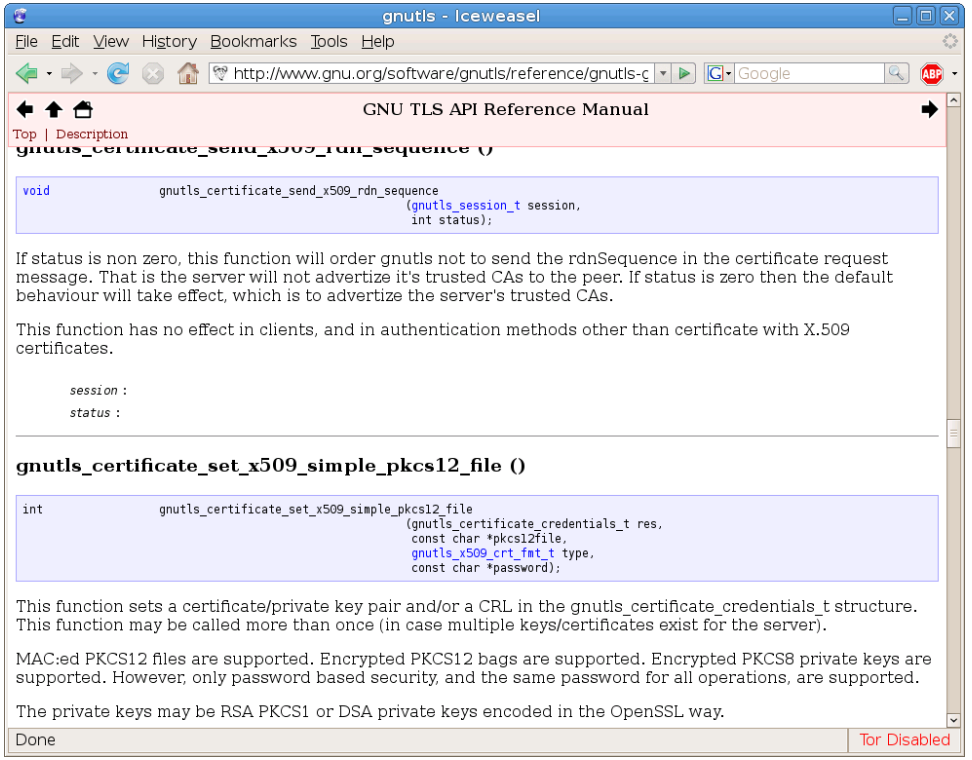
What is GnuTLS?

Reference manual





Documented source code



Official GNU project

What is GnuTLS?

libtasn1,

libgcrypt,

opencdk,

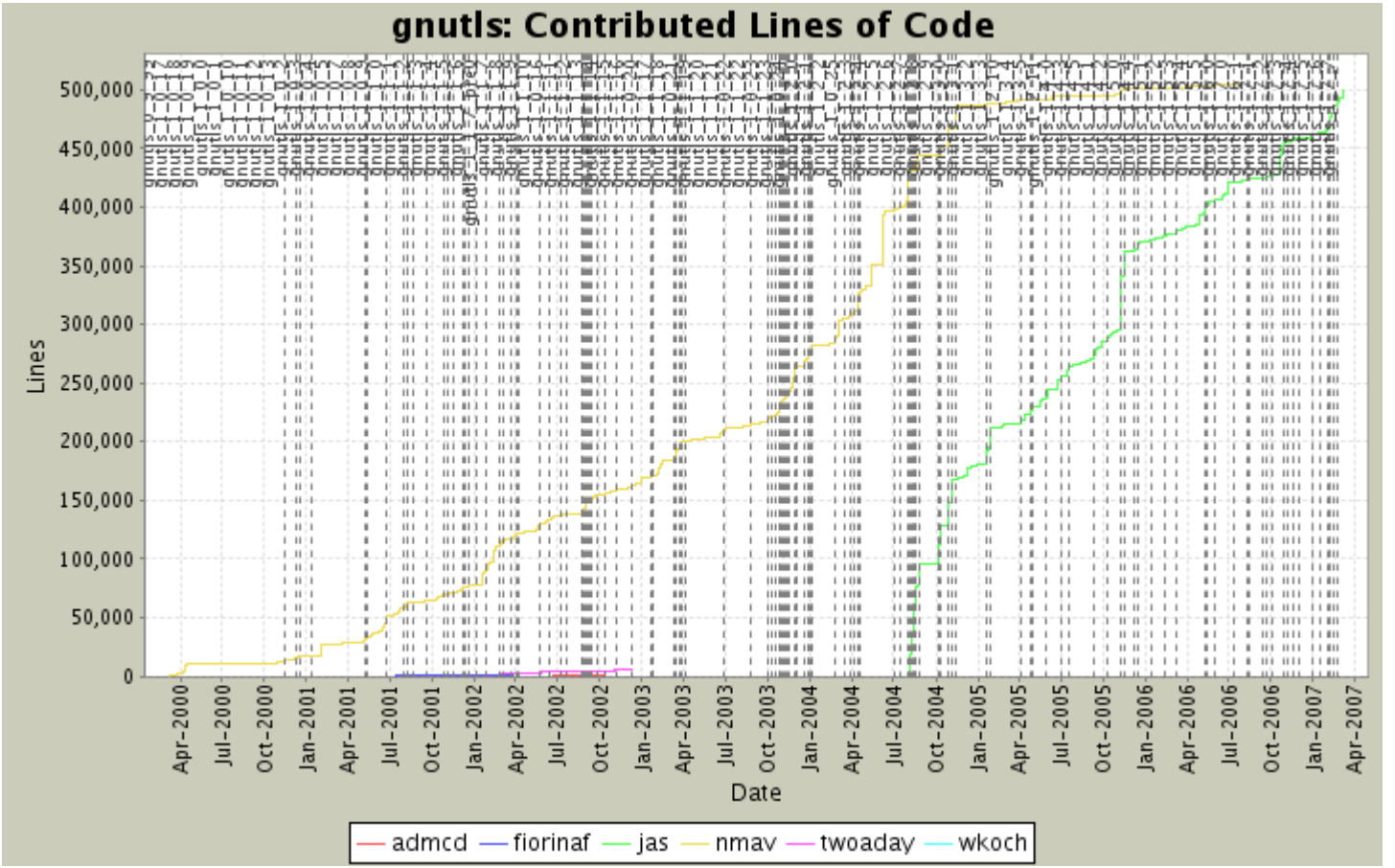
libz,

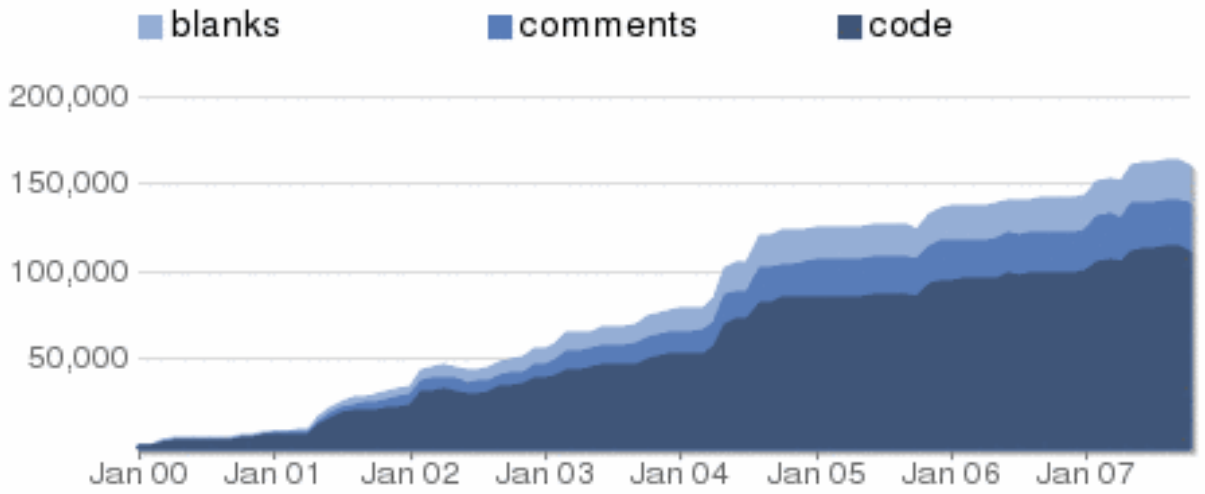
liblzo

Version control: Git
(before May 2007: CVS)

savannah.gnu.org

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!

Use your OpenPGP key during handshake

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/

mod_ssl 15kLOC
mod_gnutls 3kLOC

Support for Server Name Indication

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...**

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

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.”

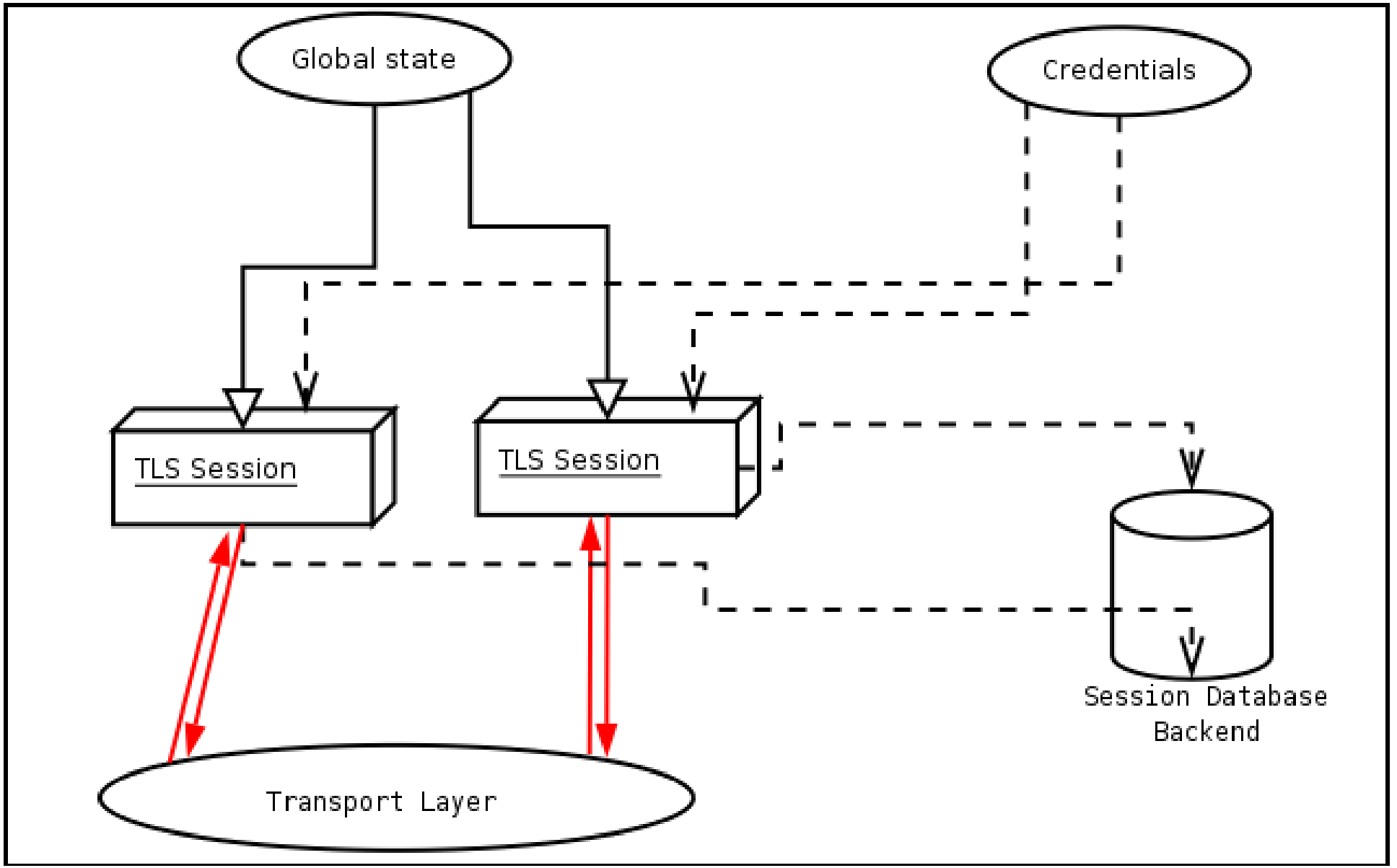
http://www.fsf.org/news/oppose-tls-authz-standard.html

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


Global state
Credentials
TLS Session
TLS Session
Session Database
Backend
Transport Layer

Questions?

Answers?

Thank you for listening!