FOSDEM '09

FREE AND OPEN SOURCE SOFTWARE DEVELOPERS' EUROPEAN MEETING

# Introduction to GnuTLS


**Simon Josefsson**

**simon@josefsson.org**

**http://josefsson.org/**


**http://www.gnutls.org/**

# What is GnuTLS?

- Implementation of Transport Layer Security
  - Provides strong encryption and authentication
  - The S in HTTPS
  - Application protocol standardized by the IETF

- Similar to OpenSSL but not does not implement non-TLS stuff like S/MIME, low-level crypto, etc

# What is GnuTLS?

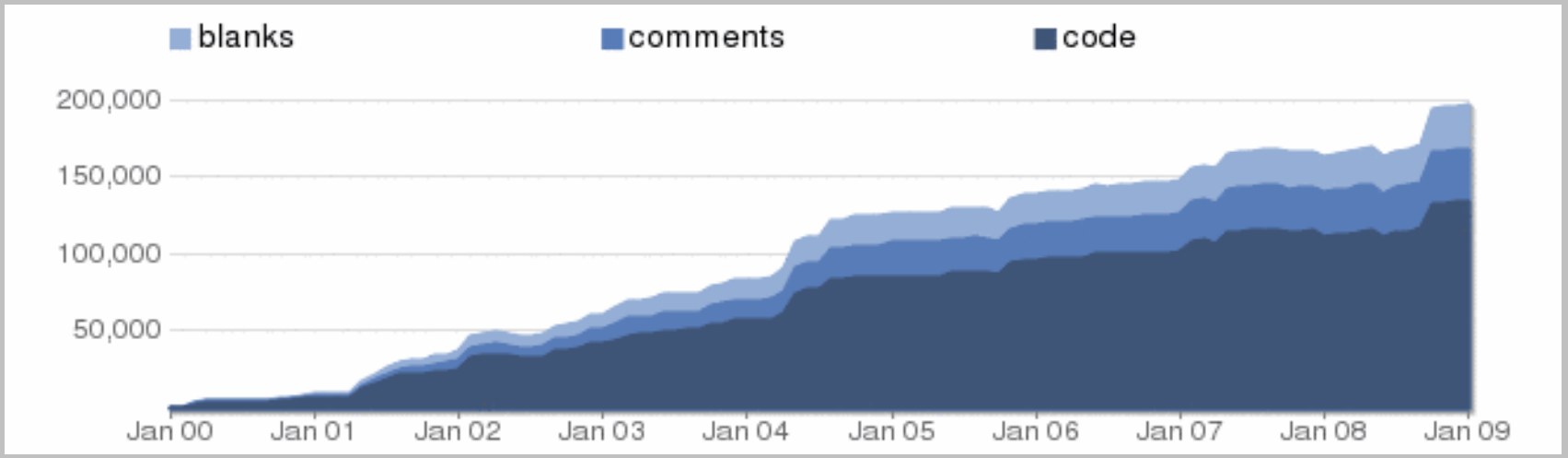
- Part of the GNU project
- Copyrights assigned to the FSF
- Core library is LGPLv2.1+, tools under GPLv3+

# What is GnuTLS?

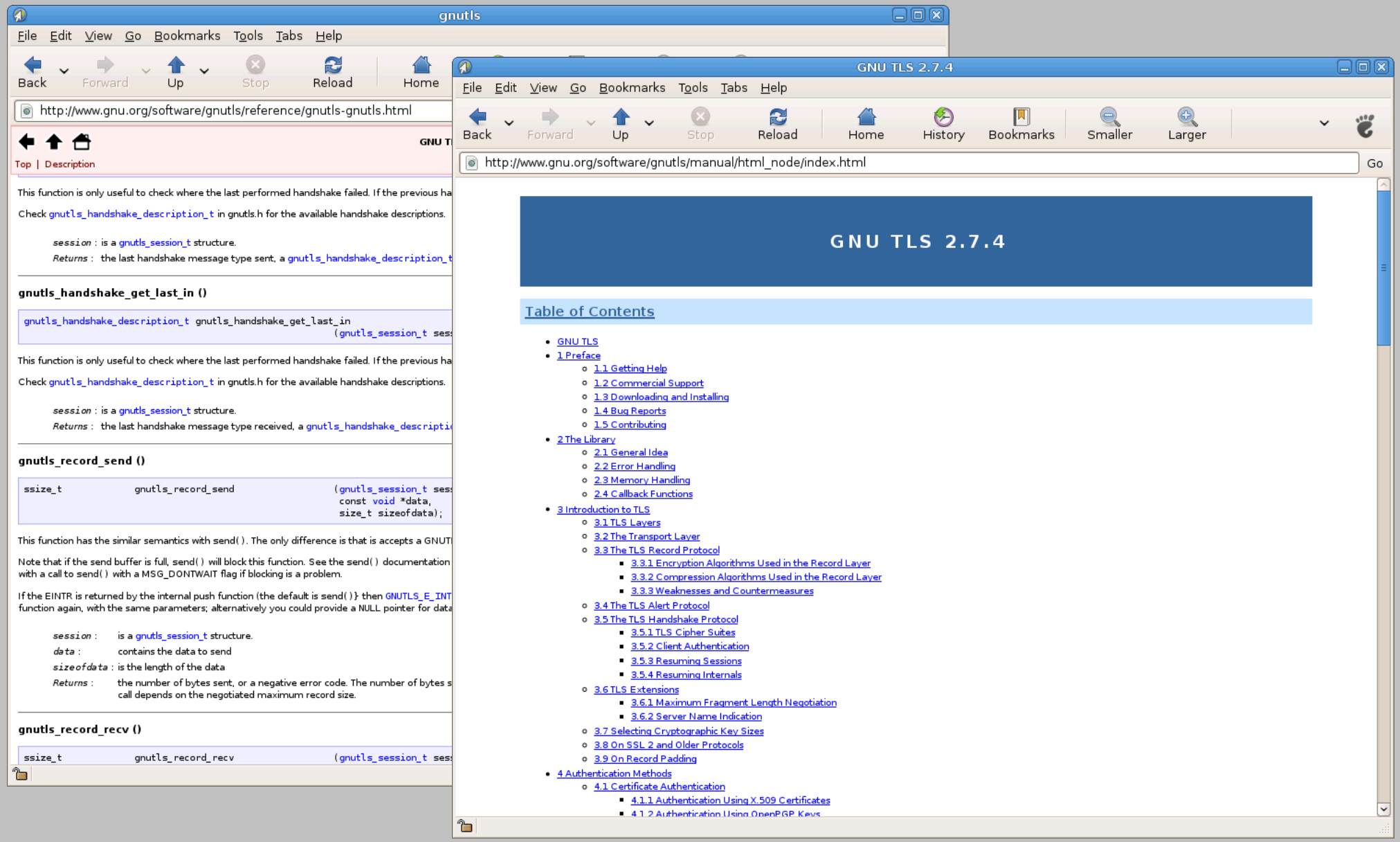
- Required dependencies:
  - Libgcrypt (replaceable), Libtasn1
- Optional dependencies
  - Libz, Liblzo (compression)
- Official API bindings for Guile and C++
- Windows installer (DLL, tools, etc) available from http://josefsson.org/gnutls4win/

# GnuTLS History

- ~8 year old project – started late 2000
- Originally written by Nikos Mavrogiannopoulos
- Currently maintained by Simon Josefsson
- Small dev team: ~15 significant contributors
- Version 1.0 in 2003 - version 2.0 in 2007

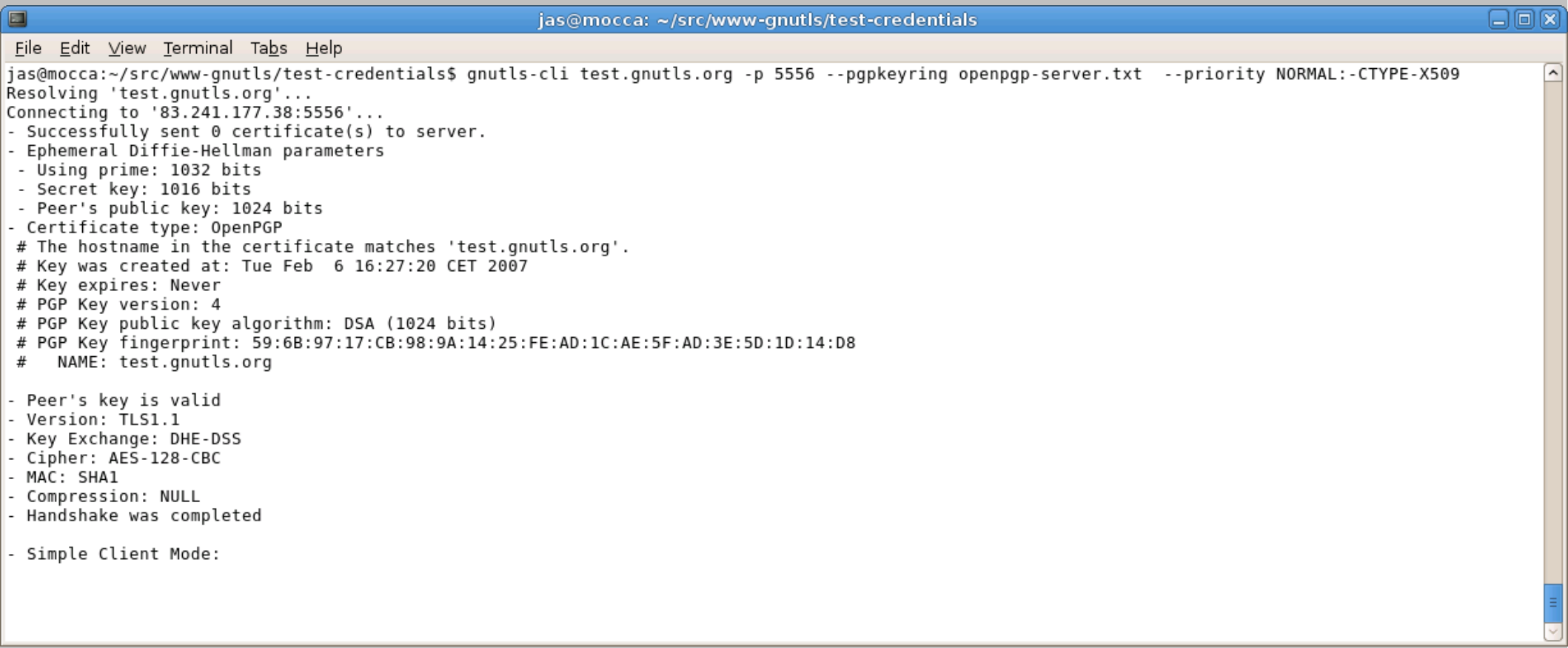


# Well documented



# Features

- Supports authentication of server and user using OpenPGP



# Features

- Strong password authentication via Secure Remote Password (SRP)
- Shared symmetric key authentication using Pre-Shared Key (PSK)
- Server Name extension
  - Used by Apache mod_gnutls
- X.509 tools to create private keys, self-signed certificates, certificate requests, etc

# Software Patent Blues

- The network security area has many overlapping patents for some techniques
- RSA the historical example, but the patent expired (and a free implementation existed)
- Secure Remote Password (SRP) is patented but freely implementable
- TLS-AUTHZ extension support in GnuTLS removed!

# The End

Thanks for listening!