C++ - Feature

C++ implementation was developed focusing and paying particular attention to mobile platforms, during the development of PrivateGSM product for Nokia and iPhone.

It has been also tested with pjsip pjsua on Windows, Linux and Mac OS X platform.

It contains:

- ZRTP protocol implementation
- SRTP protocol implementation from libsrtp svn
- Cryptographic algorithms from libtomcrypt 1.17

Mobile Optimized

Since mobile networks work in a very different way than standard broadband internet there are specific optimizations for the mobile environment:

- aggressive packet timing and retransmission to work over high latency/packet loss mobile networks

ZRTP features

Key exchange support

- DH-3072
- ECDH-256
- ECDH-384

SRTP encryption

- AES-128
- AES-256

Cache support

- Local cache
- Self-healing key continuity

Random Number Generation

- Fortuna Deterministic Random Bit Generator (DRBG)
- Microphone Audio Sample Entropy Collection

MitM detection

- Hello hash not corresponding (if SDP zrtp-hash does not match)
- Cached secret non corresponding (MITM Warning)
- Wrong HMAC

ZRTP SIP support

- SDP zrtp-hash attribute

Supported Platforms

Zorg has been tested with pjsip integration on the following platforms.

- Windows
- Symbian OS 3rd/5th edition
- iPhone OS 4
- Mac OS X
- Linux

Please note that build system could require adjustment on specific platform.