Overview

Zorg is an implementation of the ZRTP protocol. ZRTP is an in-band key exchange protocol for SRTP, based on either the Diffie–Hellman (D–H) or the elliptic curve Diffie–Hellman (ECDH) algorithms, with Man-in-the-Middle protection based on human voice recognition.
Coupled with an SRTP implementation, Zorg provides VoIP security with Diffie–Hellman (up to 3072 bits) or elliptic curve Diffie–Hellman (up to 384 bits) for key exchange, AES (up to 256 bits) for confidentiality and HMAC-SHA1 for authentication.
Zorg implementations are developed in cross-platform C++ language and Java language in order to run on most mobile phones and all desktop platforms.
Key Zorg features are:

- 100% open source
- ZRTP standard compliance
- Supported platforms:
  Blackberry, Android, iPhone, Symbian,
  Windows, Linux, MacOS X
- Language bindings for: C++, C/Objective-C, Java, J2ME MIDP 2.0
- **Modular design, especially w.r.t. cryptography suites**
- Especially optimized for mobile platforms
- Used in production in commercial grade security software
- Support ZRTP masquerading to bypass restrictive PBX that block ZRTP packets
- Made in EU - not restricted by US Export Control (but Internationally by Wassenaar Arrangement)

Zorg implements all mandatory features of ZRTP, plus key continuity and all optional Diffie–Hellman key agreement types.
In the interest of providing a minimal, secure implementation for peer-to-peer communication, Zorg doesn't implement any proxy/MitM features.
Zorg includes compatibility with LibZRTP implementation.
The project is sponsored by PrivateWave, an European (Italy) company that uses ZRTP security in its PrivateGSM voice encryption product for Blackberry, Nokia and iPhone following an open source and transparent security approach.
Please read the ZRTP page to know more about end-to-end voip encryption and find links to other online resources and other ZRTP protocol implementations.