Java - Feature

Java implementation was developed focusing and paying particular attention to mobile platforms, during the development of PrivateGSM product for Blackberry.

It contains:

- ZRTP protocol implementation
- SRTP protocol implementation

Mobile Optimized

Since mobile platforms have strict constraints on resources consumption we put great care in producing an optimized version, in order to optimize:

- encryption/digest calculations
- use efficiently memory
- aggressive packet timing and retransmission to work over high latency/packet loss mobile networks

CPU usage

Intensive CPU usage leads to battery consumption, leaving the user with a dead phone. Java implementation provides an abstraction layer to leverage on native platform encryption APIs provided by Blackberry platform (former Certicom APIs). While not done by us yet, we expect that it would be very easy and quick to add a new backend based on J2SE Crypto APIs or directly on BouncyCastle implementation.

Memory usage

Another major issue with java development is garbage collection. Every time you allocate a new Object on the heap you are producing garbage that later should be thrown away. On J2SE this is not an issue anymore, generally, but on mobile it's still a big issue that you should be aware of and worried about, particularly because mobile garbage collectors are not very efficient, eg: on blackberry JVM the GC stops the world, even for some seconds, and this is not acceptable when you are doing real-time communication!

Our implementation is particularly efficient regarding Objects reuse to reduce at minimum the GC activity.

ZRTP features

Current Java implementation is not complete ZRTP RFC draft, but it supports almost everything required to implement a secure VoIP client with end-to-end security.
Key exchange support

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

*Not working in blackberry crypto backend due to some issues with Certicom implementation
SRTP encryption

- AES-128
- AES-256

Cache support

- Local cache
- Self-healing key continuity

Random Number Generation

- Pluggable random generator, eg: 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

- Blackberry OS 4.6.x, 5.x, 6.x
- J2SE with Crypto