



## M5T Releases the M5T ZRTP SAFE Application

*The M5T ZRTP SAFE touted as the ideal solution for VoIP developers to implement the ZRTP protocol into their communications applications*



**Sherbrooke, Quebec, Canada, June 28, 2007** - M5T, the leading provider of software solutions for secure real-time multimedia communications over IP, announced today the release of the M5T ZRTP SAFE, a powerful new solution designed to perform SRTP key exchanges during call setup into the media path using the same network connection used to exchange RTP packets.

The M5T ZRTP SAFE is an effective new approach to secure VoIP because it achieves security without the reliance on a PKI (Public Key Infrastructure), key certification, trust models, certificate authorities, or key management complexity. It performs its key agreements and key management in a pure peer-to-peer manner over the RTP packet stream. It interoperates with any standard SIP phone, but naturally only encrypts the call if you are calling another ZRTP-enabled device or phone.

"In the weeks that led up to this formal release, we've heard from numerous partners excited about the possibilities of integrating our ZRTP SAFE component within their technologies," said Samuel Gu nette, General Manager for M5T. "Like all M5T SAFE Components, the M5T ZRTP SAFE integrates seamlessly with the entire line of SAFE Components including M5T SRTP SAFE and the M5T RTP SAFE."

### Key Features of the M5T ZRTP SAFE

- **Key agreement methods:** Diffie-Hellman (DH3K and DH4K);
- **No PKI required:** ZRTP does not rely on public key infrastructure (PKI) which is known to be very hard to securely deploy;
- **Seamless integration:** Fully integrated with M5T RTP SAFE and M5T SRTP SAFE;
- **Best effort encryptions:** SRTP is not always mandatory. If the peer does not support ZRTP, a user may still decide that a call should still proceed with plain RTP;
- **Perfect Forward Secrecy:** The use of ephemeral Diffie-Hellman allows perfect forward secrecy with the creation of new keys for each call. The keys are then destroyed once the call ends. A key will never be reused for another call. This feature prevents the retroactive compromise of the call by future disclosures of the key

### About M5T

M5T is a leading software provider delivering the latest in software technologies and security solutions to equipment vendors and chipset manufacturers developing applications for real-time multimedia communications over IP. The company develops middleware components based on a common framework layer, which forms the foundation for developing modular solutions. M5T is a wholly owned division of Media5 Corporation. Media5 Corporation is a high technology holding company based in Sherbrooke, Quebec, Canada. For more information please visit [www.m5t.com](http://www.m5t.com).





**M5T Contacts:**

Mike Spooner  
Marketing Communications Director  
M5T  
Tel: +1 514.402.3885  
Fax: +1.819.829.5100  
Email: [m Spooner@m5t.com](mailto:m Spooner@m5t.com)