**Voice over IP with continuous mutual authentication**

Voice over IP is a group of technologies meant to deliver voice communications over Internet, consequently there is no well-defined standard for what protocols are used in it. There are a lot of implementations for VoIP that use different protocols for each task: signalling or media transport. The most used are SIP (Session Initiation Protocol) and RTP (Real-time Transport Protocol).

Security is a big concern for VoIP as confidentiality and authentication are wanted features for a conversation between parties. Solutions today include a protocol developed in 2004 – SRTP (Secure RTP) which provides symmetric encryption for packets and authentication using an authentication tag for each packet. Also, ZRTP (Zimmerman RTP) is used for key establishment for a SRTP session. While these protocols work well together, they are not suitable for devices with low computational power, such as stationary phones. We need to find an alternative that would offer good security while being fast and lightweight.

In 2011, a new technology for security was developed, namely Real Privacy Management (RPM) by Relevant Security Corp., which offers a fast cryptographic scheme for continuous mutual authentication. The solution is based on modular arithmetic and several position digit algebra functions. The digit manipulations make the functions fast and allow for parallel processing.

To use a similar solution as RPM in VoIP, we need to consider similarities and differences between it and the solutions used today. Both SRTP and RPM use symmetric cryptography, therefore they need a mechanism for master key establishment. Also, RPM uses pre-shared secrets, similar for both parties and does not provide a way to generate and distribute them. This requirements can be met by using ZRTP as the key establishment mechanism. So that at each session the parties check whether they have shared secrets stored in memory, and use them if they do, otherwise establish new ones using ephemeral-key Diffie-Hellman method from ZRTP.

At each message exchange between parties, the shared secrets update in a symmetric way individually for each party and used to determine the encryption key used in AES, thus providing continuous mutual authentication, as only the legitimate participants know the pre-shared secrets used.