



**SURVEY ARTICLE**

## **A Survey and Analysis of Media Keying Techniques in Session Initiation Protocol (SIP)**

**Rajesh Kumar<sup>1</sup>, Sandip Chauhan<sup>2</sup>**

<sup>1</sup>Kalol Institute of Technology affiliated to G.T.U., Ahmadabad, India

<sup>2</sup>Kalol Institute of Technology affiliated to G.T.U., Ahmadabad, India

---

*Abstract— In this paper we are presenting a survey about the key exchange protocols namely ZRTP, DTLS-SRTP, SDES[4] and MSDES[15]. The SIP is used for signaling in VOIP which is completely text based application layer protocol hence there is a lot of security issues and challenges associated with VOIP. A detailed analysis of key exchange protocols and its suitability with SIP has been carried out in this paper.*

*In VOIP we require security at both signaling and data transfer levels and signaling is text based so confidentiality of signaling parameters and data is a big challenge in VOIP. Even exchanging cryptographic keys to encrypt the media stream in the SIP is difficult task. There is a need for stronger key management protocols which will secure the voice data from various types of attack and which also provides a feasible key exchange mechanism.*

***Key Terms: - SIP; key exchange; media; security; SDES; ZRTP; DTLS; MSDES; SRTP***

---