

## Abstract

*IP Multimedia Subsystem (IMS) is one of the server system handle a number of services, one of the service is VoIP (Voice over Internet Protocol). In the implementation, VoIP is transmitted through the Realtime Transport Protocol (TLS), which incidentally does not have the strength in terms of security. Accordingly, then present a number of methods used to secure , especially from sniffing action (tapping), with Session Description Protocol Security Descriptions (SDS).*

*SDS secures RTP by exchanging a symmetric key, so that only the end-user who has can encrypt and decrypt messages transmitted and received voice. However, to be able to perform key exchange, there should be a protocol that ensures safety during the key exchange. Therefore the TLS protocol is used.*

*This final report contains discussion of the process that happens on SDS when a client of non-IMS server exchanges key with client from non-IMS server, in this case is Asterisk server. Then do the testing security against sniffing action.*

*Based on the test results obtained that SDS can protect voice messages transmitted optimally despite passing between different server, and it has nearly the same invite time the network that does not implement SDS.*

**Key words:** *a crypto, invite time, TLS, VoIP*