



## SRTP (Secure Real-time Transport Protocol)

VOCAL's embedded software libraries include a complete range of ETSI / ITU / IEEE compliant algorithms, in addition to many other standard and proprietary algorithms. Our software is optimized for execution on ANSI C and leading DSP architectures (TI, ADI, AMD, ARM, CEVA, LSI Logic ZSP, and MIPS). These libraries are modular and can be executed as a single task under a variety of operating systems or standalone with its own microkernel.

The Secure Real-time Transport Protocol (SRTP) defines a framework which provides confidentiality, message authentication, and replay protection for both unicast and multicast RTP and RTPCP streams. SRTP is very suitable for VoIP applications, especially those involving low-bitrate voice codecs (i.e. G.729, iLBC, MELP, etc.) since it can be used with header compression and has no significant impact on Quality of Service. It can also be used to with JPEG, MPEG2, and MPEG4 to securely stream video in multimedia applications. SRTP can achieve high throughput and low packet expansion even in environments that are a mixture of wired and wireless networks.

SRTP is the security layer which resides between the RTP/RTCP application layer and the transport layer, generating SRTP packets from the RTP/RTCP stream and forwarding these to the receiver. Similarly, it also transforms incoming SRTP packets to RTP/RTCP packets and passes these up the stack. The cryptographic state information associated with each SRTP stream is termed the cryptographic context. It must be maintained by both the sender and receiver of SRTP streams. If there are several SRTP streams present within a given RTP session, separate cryptographic contexts must be maintained for each. A cryptographic context includes any session key (a key directly in encryption/message authentication) and the master key (a securely exchanged random bit string used to derive session keys), as well as other working session parameters.

While SRTP does not define a precise mechanism to implement key exchange, it does provide for several features which make key management easier and heighten overall key security. The single master key is used to provide keying material for a key derivation function. This can generate the initial session keys, as well as provide new session keys periodically to ensure that there will be a limited amount of ciphertext produced by any given encryption key. Salting keys are used to provide protection against various assaults such as pre-computation and time-memory attacks.

### Features

- Compliant with Secure Real-time Transport Protocol [RFC 3411](#)
- Various encryption libraries available
- Secure RTP/RTCP payloads
- Ensure integrity of RTP/RTCP payloads
- Protect against replayed packet attack
- Low bandwidth implementation
- Low computational cost and small footprint
- Independent of network and physical layers

---

**VOCAL Technologies Ltd.**  
90A John Muir Drive  
Buffalo, New York  
14228

<http://www.vocal.com>  
[Email: sales@vocal.com](mailto:sales@vocal.com)  
Tel: 716-688-4675  
Fax: 716-639-0713