

Features

- Compliant with Secure Real-time Transport Protocol RFC 3711
- Secures RTP/RTCP payloads
- Integrity checking of RTP/RTCP payloads
- Implements packet transform required by in SRTP/SRTCP
- Low computational cost and small footprint
- Independent of transport and physical layers
- Hardware offload supported
- Optional support for Master Key Identifier (MKI)
- Licensed in C source code to facilitate porting to the target system

The Secure Real-time Transport Protocol (SRTP) defines a framework which provides confidentiality, message authentication, and replay protection for both unicast and multicast RTP (Real-time Transport Protocol) and RTCP (Real-time Transport Control Protocol) streams used for voice and video transmission over the Internet

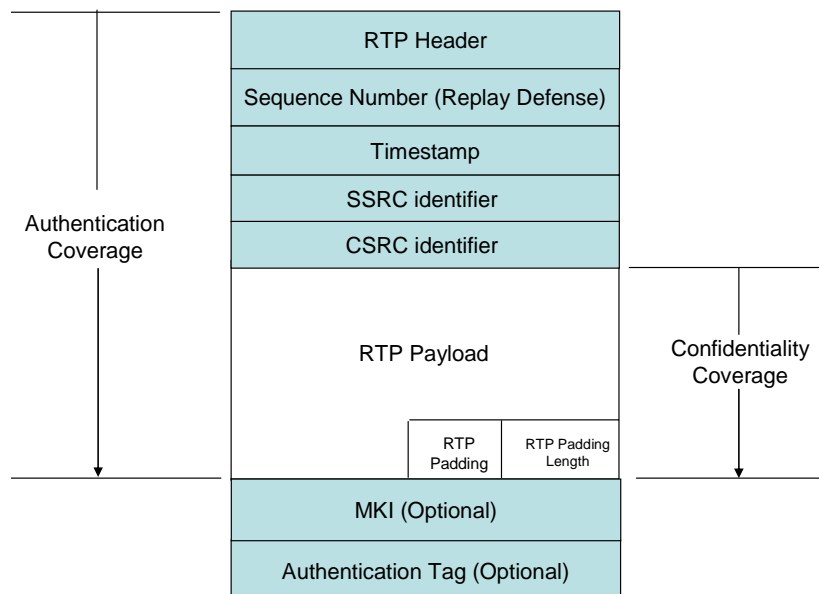
The ESS-05 Ellipsys-SRTP Toolkit offers a software toolkit which facilitates the implementation of SRTP systems ranging from low bit rate voice over IP (VoIP) applications to high-definition video streaming. The ESS-05 offers the option to implement either an all software solution using the ESS-01 Ellipsys software library or when hardware cores are available in the target system, offload can be supported through a Board Support Package (BSP). The toolkit was developed on a Linux/PC environment, has been ported to a Freescale PowerQUICC III processor and is licensed as C source code.

General Description

Overview of SRTP

The Secure Real-time Transport Protocol defines a framework which provides confidentiality, message authentication, and replay protection for both unicast and multicast RTP (Real-time Transport Protocol) and (RTCP Real-time Transport Control Protocol) streams. SRTP is used in voice over VoIP applications and video for MPEG-4 or H.264 encoded streams. The ESS-05 SRTP toolkit enables system developers to achieve high throughput over wired and wireless networks.

SRTP is a security layer that resides between the RTP/RTCP application layer and the transport layer, generating SRTP packets from the RTP/RTCP stream and forwarding them to the receiver. Similarly, it also transforms incoming SRTP packets to RTP/RTCP packets and passes them up the stack. The SRTP transform is shown in the figure below.



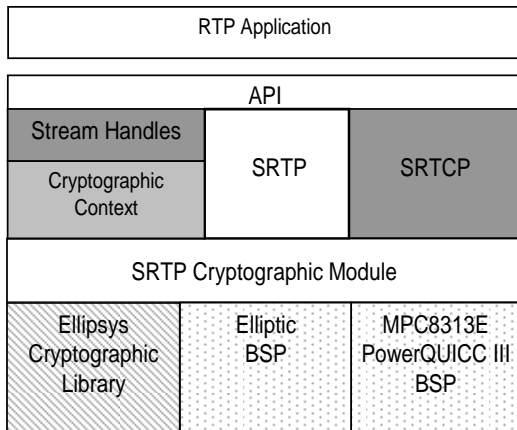
General Description cont'

SRTP support two ciphers – AES in counter mode (AES-CTR) and AES-f8. Integrity checking is done using the HMAC-SHA-1 algorithm. Both of these cipher suites are supported in the ESS-05 either in software or through hardware offload engines when available.

RFC3711 does not specify a key management protocol although the standard suggests a number of emerging options that can be used in SRTP applications such as MIKEY, KEYMGMT and SDMS.

Key management is therefore not implemented in the ESS-05 but it does store the required cryptographic contexts (keys, initialization vectors, salts, lifetime, etc.) for the cipher and integrity algorithms and associates them with

RTP stream handles. Security protocols also specify re-keying which is designed to make hacking the security design much more difficult. Re-keying in the ESS-05 is supported through the Master Key Identified (MKI) and MKI-Rekeying functions available in the toolkit.



Overview of the ESS-05 SRTP Toolkit

The block diagram of the ESS-05 is shown in Figure 2. The components of the software system include:

1. An API which allows the RTP application to manage SRTP and SRTCP context structures.
2. Stream handles which maps RTP streams to security contexts.
3. The SRTP module which encodes RTP packets before they are sent to the transport layer and decodes SRTCP packets received from the transport layer.
4. The SRTCP module which encodes RTCP packets before they are sent to the transport layer and decodes SRTCP packets received from the transport layer.
5. The SRTP Cryptographic module provides cryptographic functions in support of the RTP transform specified in RFC3711.
6. The Ellipsys Crypto Library provides the software ciphers and hashes required for the security transforms.
7. The optional BSP for Elliptic hardware provides support for cores if available in the target silicon; and
8. The optional MPC8313E PowerQUICC BSP provides an interface to the PowerQUICC III SEC offload engine.

Elliptic developed the ESS-05 Ellipsys-SRTP Toolkit in a Linux/PC environment using Fedora Linux. The toolkit has been successfully ported to Freescale Linux 2.6.28 for the MPC8313E processor.

Ordering Information

- The ESS-05 is licensed in ANSI C source code and is available for immediate delivery.