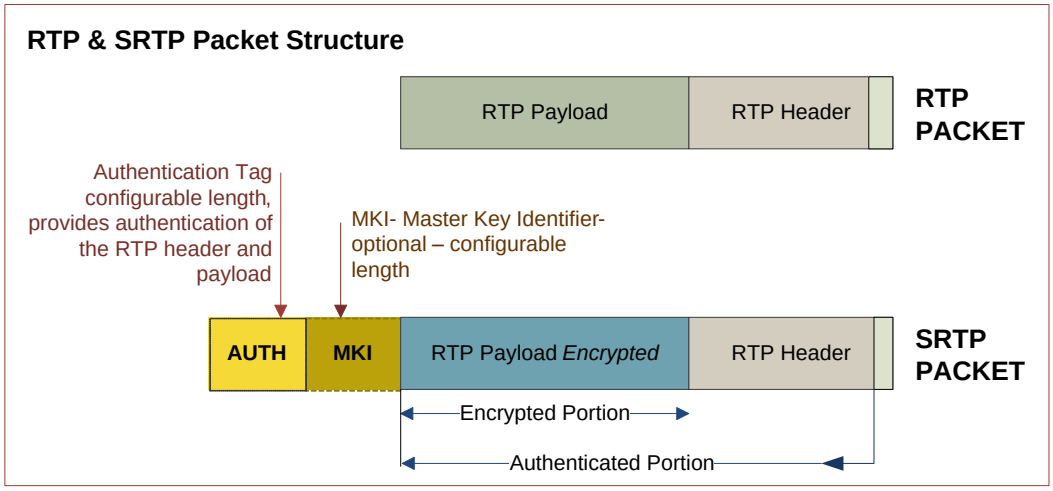
Adaptive Digital Technologies, Inc.

SRTP Series

SRTP is a security profile for RTP that adds confidentiality, message authentication, and replay protection to that protocol. SRTP is ideal for protecting Voice over IP traffic because it has no effect on voice quality and payload overhead is only minimally affected.



PRODUCT DESCRIPTION

SRTP, SRTCP*, & SRTCP-XR*[*] are not separate protocols but are profiles of RTP. When security is being used, the packet payloads are encrypted.

RTP is specifically designed to handle the play-out requirements of real-time media streams through the use of time stamps and jitter buffering. Due to the real-time nature of the data streams, where requesting retransmissions is too costly in time, RTP is typically used in conjunction with UDP to provide low-overhead network communications between two end-points.

RFC 3550 identifies two components to the real-time transport: data transport and control. Data transport is handled by RTP while Real Time Control Protocol (RTCP) handles control. RTCP, which can be used to help scale the network traffic to the available bandwidth, is optional.

An RTP packet identifies the media payload type (format) and its source. It also includes time stamps and sequence numbers that are used by the play-out side to handle lost or out of sequence packets. RTP provides for the use of multiple streams as in the case of a system that transmits both voice and video. The payload in an RTP payload contains the encoded voice or video information. The use of dynamically defined payload types allows RTP packets to carry virtually any type of media format.

A secure transmission feature, as defined in IETF RFC 3711 is also available for these protocols. When security is used, the packet payloads are encrypted, an “S” prefaces the acronyms: SRTP, SRTCP, SRTCP-XR.

[*] Adaptive Digital currently does not support RTCP.

FEATURES

- Multi-channel capable.
- Functions are C-callable.
- Secure variants include support for:
  - Authentication Algorithm Types: HMAC-SHA1 and MD5
  - Key Definition Schemes: PSK, MKI, and FT
- Encryption Algorithm Types: AES - CM, AES - F8
- Supports multiple SRTP streams with same or different peers simultaneously.
- Master key used to derive session keys.
- SRTP (Secure RTP) conform to IETF RFC 3711.
- eXpressDSP™ Algorithm Interoperability Standard (xDIAS) Compliant

AVAILABILITY

ADT **SRTP** is a secure transmission feature, as defined in IETF RFC 3711. ADT SRTP is available in transportable "C" source code format as well as in library object format on all the Texas Instruments TMS320™ DSPs, and TNETV™ family of VoIP processors, ARM Cortex-A8/9/15, and ARM9E.

Product	Platform	Memory Model	Endian	Code Gen Tool Version
ADT_ srtp_c64xp/c674x/c66x	TI TMS320C64x+/C674x/C66x	L3	Little	N/R
ADT_ srtp_c64x	TI TMS320C64x	L3	Little	N/R
ADT_srtp_c55x	TI TMS320C55x	Large	Little	N/R
ADT_srtp_c54x	TI TMS320C54x	Far	N/A	N/R
ADT_ srtp_cortex-a8/a9/a15	ARM Cortex-A8/A9/A15	N/A	Little	gcc 4.6.1
ADT_ srtp_cortex-arm9e	ARM9E	N/A	Little	gcc 4.6.1

SPECIFICATIONS

CPU UTILIZATION

Peak CPU utilization occurs when a new master encryption key is required. Normal voice over IP applications require only a single key for the duration of a conversation; in this case, the peak occurs only at the start of an RTP stream.

TI TMS320C6000

C64x+ MIPS

Payload Size (Bytes/10 msec)	Options	Frame Rate (msec)					
		10		20		30	
		Avg	Peak	Avg	Peak	Avg	Peak
10	Encrypt	.31	1.75	.29	.99	.19	.67
	Decrypt	.32	1.75	.29	1.00	.20	.67
	Encrypt+Auth	.97	2.41	.61	1.32	.42	.89
	Decrpyt+Auth	.98	2.40	.62	1.33	.42	.89
80	Encrypt	1.36	2.78	1.34	2.05	1.33	1.81
	Decrypt	1.38	2.80	1.35	2.06	1.34	1.81
	Encrypt+Auth	2.16	3.58	1.81	2.52	1.73	2.20
	Decrpyt+Auth	2.18	3.59	1.82	2.52	1.74	2.21

C64x MIPS

Payload Size (Bytes/10 msec)	Options	Frame Rate (msec)					
		10		20		30	
		Avg	Peak	Avg	Peak	Avg	Peak
10	Encrypt	.33	1.82	.30	1.04	.20	.70
	Decrypt	.34	1.80	.30	1.03	.21	.69
	Encrypt+Auth	.99	2.48	.63	1.37	.42	.92
	Decrpyt+Auth	1.00	2.46	.64	1.36	.43	.91
80	Encrypt	1.38	2.87	1.35	2.09	1.34	1.83
	Decrypt	1.40	2.85	1.36	2.10	1.34	1.83
	Encrypt+Auth	2.18	3.66	1.82	2.56	1.74	2.23
	Decrpyt+Auth	2.20	3.65	1.83	2.55	1.75	2.23

TI TMS320C5000

C55x MIPS

Payload Size (Bytes/10 msec)	Options	Frame Rate (msec)					
		10		20		30	
		Avg	Peak	Avg	Peak	Avg	Peak
10	Encrypt	2.98	15.57	2.94	9.22	1.96	6.15
	Decrypt	3.0	15.59	2.95	9.23	1.97	6.15
	Encrypt+Auth	4.17	16.76	3.54	9.81	2.36	6.54
	Decrpyt+Auth	4.20	16.62	3.55	9.83	2.37	6.55
80	Encrypt	14.58	27.24	14.54	20.81	14.53	18.66
	Decrypt	14.6	27.09	14.55	20.82	14.54	18.73
	Encrypt+Auth	16.04	28.51	15.4	21.66	15.27	19.45
	Decrpyt+Auth	16.07	28.71	15.4	21.67	15.28	19.46

C54x MIPS

Payload Size (Bytes/10 msec)	Frame Rate (msec)	Encrypt		Encypt+Auth		Decrypt		Decypt+Auth	
		Avg	Peak	Avg	Peak	Avg	Peak	Avg	Peak
10	10	0.84	5.34	2.83	7.29	.086	5.36	2.87	7.36
	20	0.80	3.04	1.80	4.03	0.82	3.07	1.82	4.07
	30	0.54	2.03	1.21	2.70	0.55	2.05	1.22	2.72
80	10	3.91	8.38	6.35	10.84	3.94	8.43	6.38	10.85
	20	3.88	6.12	5.32	7.57	3.89	6.13	5.35	7.58
	30	3.87	5.36	5.12	6.62	3.88	5.37	5.14	6.63

MEMORY REQUIREMENTS The SRTP APIs are re-entrant and may be shared by multiple streams running in multiple processing threads.

TI TMS320C6000

C64x+ All Memory usage is given in units of byte.

Memory Type	Usage	Alignment
Shared Program	32,00	N/A
Shared Data	870	N/A
Per-Thread Scratch	320	N/A
Per-Channel Context Send	840	8 byte
Per-Channel Context Receive	864	8 byte

C64x All Memory usage is given in units of byte.

Memory Type	Usage	Alignment
Shared Program	38,200	N/A
Shared Data	870	N/A
Per-Thread Scratch	320	N/A
Per-Channel Context Send	840	8 byte
Per-Channel Context Receive	864	8 byte

TI TMS320C5000

C55x All Memory usage is given in units of byte.

Memory Type	Usage	Alignment
Shared Program	16,677	N/A
Shared Data	1696	N/A
Per-Thread Scratch	320	N/A
Per-Channel Context Send	1300	8 byte
Per-Channel Context Receive	1324	8 byte

C54x All Memory usage is given in units of 16-bit word.

Memory Type	Usage
Shared Program	8963
Shared Data	2202
Per-Thread Scratch	160
Per-Channel Context Send	572
Per-Channel Context Receive	584

ARM® DEVICES

ARM/ Cortex-A8

MEMORY REQUIREMENTS (All Memory usage is given in units of bytes.)

Memory Type	Usage	Alignment
Shared Program	45264	N/A
Shared Data	2240	N/A
Per-Thread Scratch	320	N/A
Per-Channel Context Send	840	8 byte
Per-Channel Context Receive	864	8 byte

CPU UTILIZATION

Payload Size (Bytes/10 msec)	Options	Frame Rate (msec)		
		10 Avg	20 Avg	30 Avg
10	Encrypt	0.6	1.1	1.2
	Decrypt	0.9	1.1	1.1
	Encrypt+Auth	1.3	1.8	1.8
	Decrpyt+Auth	1.3	1.8	1.8
80	Encrypt	2.6	5.1	7.6
	Decrypt	2.6	5.2	7.6
	Encrypt+Auth	3.6	6.1	8.8
	Decrpyt+Auth	3.5	6.1	8.9

ARM/ AMR9E

MEMORY REQUIREMENTS (All Memory usage is given in units of bytes.)

Memory Type	Usage	Alignment
Shared Program	43292	N/A
Shared Data	2192	N/A
Per-Thread Scratch	320	N/A
Per-Channel Context Send	840	8 byte
Per-Channel Context Receive	864	8 byte

CPU UTILIZATION

Payload Size (Bytes/10 msec)	Options	Frame Rate (msec)		
		10 Avg	20 Avg	30 Avg
10	Encrypt	0.6	1.2	1.1
	Decrypt	0.7	1.1	1.1
	Encrypt+Auth	1.2	1.7	1.7
	Decrpyt+Auth	1.3	1.6	1.7
80	Encrypt	2.5	5.0	7.4
	Decrypt	2.7	5.0	7.4
	Encrypt+Auth	3.3	5.8	8.5
	Decrpyt+Auth	3.3	5.8	8.5

TERMINOLOGY

RTP - Real-time Transport Protocol

SRTP - Secure Real-time Transport Protocol

AES - Advanced Encryption Standard

AES CM - Advanced Encryption Standard counter mode

AES-f8 - AES in f8-mode, Universal Mobile Telecommunications System (UMTS) 3G mobile networks use AES-f8.

AES CBC - Advanced Encryption Standard Cipher-block chaining

MKI - Master key identifier

HMAC - Hashed message authentication

MD5 - Message Digest 5 *is a widely used cryptographic hash function with a 128-bit hash value*

Deliverables

The deliverable items are platform dependent. In general, there is one library. (Sometimes multiple variants of the library are included in the deliverables.) There are also header files, some of which are specific to the product and others are common across many of Adaptive Digital's products. Also included in the deliverables is product documentation, which includes a users guide and usually includes release notes and a data sheet. Sample/test code may be included as well.

Adaptive Digital is a member of the Texas Instruments Developer Network, and ARM Connected Community.

CONTACT INFORMATION

Web: www.adaptivedigital.com
Email: information@adaptivedigital.com
Tel: 610.825.0182
Fax: 610.825.7616
Address: 525 Plymouth Road, Suite 316
Plymouth Meeting, PA 19462

TEXAS INSTRUMENTS
TI Developer Network

ARM CONNECTED

ADAPTIVE DIGITAL TECHNOLOGIES

