Contents

[1 Introduction 2](#_Toc364157560)

[1.1 Revision history 2](#_Toc364157561)

[1.2 How to Read this Document 2](#_Toc364157562)

[1.3 Scope 2](#_Toc364157563)

[1.4 References 2](#_Toc364157564)

[1.5 Abbreviations 2](#_Toc364157565)

[1.6 Terminology 2](#_Toc364157566)

[2 General 3](#_Toc364157567)

[3 Functional specification 3](#_Toc364157568)

[3.1 Protocol version implemented 3](#_Toc364157569)

[3.1.1 Protocol Modifications/Deviations 3](#_Toc364157570)

[3.2 Encoding/Decoding and Other Related Functions 4](#_Toc364157571)

# Introduction

## Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Rev | Characteristics | Prepared |
| 2013-03-27 | PA1 | First draft version | EZOLMED |
| 2013-08-07 | PB1 | HR60837 has been implemented. | EZOLMED |
|  |  |  |  |

## How to Read this Document

This is the Function Specification for the set of SRTP protocol modules. SRTP protocol modules are developed for the TTCN-3 Toolset with TITAN. This document should be read together with Product Revision Information [2].

## Scope

The purpose of this document is to specify the content of the SRTP protocol modules. Basic knowledge of TTCN-3 [1] and TITAN TTCN-3 Test Executor [3] is valuable when reading this document.

## References

1. ETSI ES 201 873-1 V.4.4.1 (2012-04) The Testing and Test Control Notation version 3 Part 1: Core Language
2. 109 21-CNL 113 769-1 Uen SRTP ProtocolModules for TTCN-3 Toolset with TITAN, Product Revision Information
3. 1/198 17-CRL 113 200/3 Uen - User Guide for TITAN TTCN–3 Test Executor
4. IETF RFC 3711

## Abbreviations

TTCN-3 Testing and Test Control Notation version 3

SRTP Secure Real-time Transport Protocol

## Terminology

No specific terminology is used.

# General

Protocol modules implement the message structures of the related protocol in a formalized way, using the standard specification language TTCN-3 [1]. This allows defining of test data (templates) in the TTCN-3 language [2] and correctly encoding/decoding messages when executing test suites using the Titan TTCN-3 test environment [3].  
Protocol module is using encoding attributes and hence is usable with the Titan test toolset only.

# Functional specification

## Protocol version implemented

This set of protocol modules implements protocol messages and constants of the SRTP protocol.

### Protocol Modifications/Deviations

None.

## Encoding/Decoding and Other Related Functions

This product also contains encoding/decoding [4] functions which assure correct encoding of messages when sent from Titan and correct decoding of messages when received by TITAN. Implemented encoding/decoding functions:

Name Type of formal parameters

|  |  |
| --- | --- |
| ef\_SRTP\_enc\_pdu | in RTP\_messages\_union pl\_pdu,  **out octetstring pl\_result**,  in BIT32\_BO\_LAST pl\_first\_ssrc,  in Key\_Generators pl\_generators, (session key and salt record)  in Srtp\_Crypto\_Transform pl\_srtp\_crypto\_transform := SRTP\_AES\_CM,  in Srtp\_Crypto\_Hash pl\_srtp\_crypto\_hash := SRTP\_HMAC\_SHA1 |
| ef\_SRTP\_dec\_pdu | in octetstring pl\_stream,  **out RTP\_messages\_union pl\_pdu,**  in BIT32\_BO\_LAST pl\_first\_ssrc,  in Key\_Generators pl\_generators , (session key and salt record)  in Srtp\_Message\_Types pl\_message\_type, (RTP or RTCP message)  in Srtp\_Crypto\_Transform pl\_srtp\_crypto\_transform := SRTP\_AES\_CM,  in Srtp\_Crypto\_Hash pl\_srtp\_crypto\_hash := SRTP\_HMAC\_SHA1 |