|  |  |
| --- | --- |
|  |  |

IPsec protocol module for TTCN-3 Toolset with TITAN, Function Description

# Abstract

The purpose of this document is to specify the functionality and usage of the IPsec protocol module.

Contents

[1 Introduction 2](#_Toc391540865)

[1.1 Revision history 2](#_Toc391540866)

[1.2 How to Read this Document 2](#_Toc391540867)

[1.3 Scope 2](#_Toc391540868)

[1.4 References 2](#_Toc391540869)

[1.5 Abbreviations 2](#_Toc391540870)

[1.6 Terminology 3](#_Toc391540871)

[1.7 System Requirements 3](#_Toc391540872)

[1.8 Installation 3](#_Toc391540873)

[1.9 Configuration 3](#_Toc391540874)

[2 Functional specification 3](#_Toc391540875)

[2.1 Protocol version implemented 3](#_Toc391540876)

[2.1.1 Implemented encoding/decoding functions: 3](#_Toc391540877)

# Introduction

## Revision history

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Rev | Characteristics | Prepared |
| 2018-06-11 | PA1 | First draft version | EESZSUS |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## How to Read this Document

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

## Scope

The purpose of this document is to specify the content of the IPsec protocol module. Basic knowledge of TTCN-3 [2] and TITAN TTCN-3 Test Executor [5] is valuable when reading this document.

## References

#### RFC 4303 IP Encapsulating Security Payload

1. ETSI ES 201 873-1 v4.5.1 (2013-02)  
   The Testing and Test Control Notation version 3; Part 1: Core Language
2. 109 21-CNL 113 809-1 Uen  
   IPsec Protocol Module for TTCN-3 Toolset with TITAN, Product Revision Information
3. 2/198 17-CRL 113 200/4 Uen  
   Programmer’s Technical Reference for the TITAN TTCN-3 Test Executor
4. 1/198 17-CRL 113 200/4 Uen  
   User Guide for the TITAN TTCN-3 Test Executor

## Abbreviations

ESP Encapsulating Security Payload

IPsec Internet Protocol Security

TTCN-3 Testing and Test Control Notation version 3

ETSI European Telecommunications Standards Institute

ITU-T International Telecommunication Union – Telecommunication Standardization Sector

## Terminology

No specific terminology is used.

## System Requirements

Protocol modules are a set of TTCN-3 source code files that can be used as part of TTCN-3 test suites only. Hence, protocol modules alone do not put specific requirements on the system used. However in order to compile and execute a TTCN-3 test suite using the set of protocol modules the following system requirements must be satisfied:

* TITAN TTCN-3 Test Executor version R8A (1.8.pl0) or higher installed. Please note: This version of the protocol module is not compatible with TITAN releases earlier than R8A.

## Installation

The set of protocol modules can be used in developing TTCN-3 test suites using any text editor. However to make the work more efficient a TTCN-3-enabled text editor is recommended (e.g. nedit, xemacs). Since the IPsec protocol is used as a part of a TTCN-3 test suite, this requires TTCN-3 Test Executor be installed before the module can be compiled and executed together with other parts of the test suite. For more details on the installation of TTCN-3 Test Executor see the relevant section of [4].

## Configuration

None.

# Functional specification

## Protocol version implemented

This set of protocol modules implements protocol messages, constants and encode/decode functions of the IPsec ESP protocol. The module is based on RFC 2406 (see [1]). The following messages are implemented:

ESP\_Message

ESP\_Data

### Implemented encoding/decoding functions:

Name Type of formal parameters

ef\_ESP\_encode in ESP\_Message pl\_pdu,

return octetstring pl\_stream

ef\_ESP\_decode in octetstring pl\_stream, in integer pl\_auth\_length

out ESP\_Message pl\_pdu

return integer

ef\_ESP\_Cipher\_Data\_encode in ESP\_Data pl\_payloads,

return octetstring pl\_stream

f\_ESP\_Cipher\_Data\_decode in octetsring pl\_stream,

out ESP\_Data

return ESP\_Message pl\_pdu