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

Eszter Susánszky

Version 1551-CNL 113 809, Rev. A, 2014-06-26

Table of Contents

How to Read this Document . . . 1
Scope . . . 1
System Requirements . . . 1
Installation . . . 1
Configuration . . . 1
Functional Specification . . . 1
    Protocol Version Implemented . . . 1
        Implemented Encoding/Decoding Functions: . . . 2
Terminology . . . 2
Abbreviations . . . 2
References . . . 3

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.

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 [4] is valuable when reading this document.

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.

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 [3].

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). 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

Terminology

No specific terminology is used.

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

References

[1] RFC 4303
IP Encapsulating Security Payload

[2] ETSI ES 201 873-1 v4.5.1 (2013-02)
The Testing and Test Control Notation version 3; Part 1: Core Language

[3] Programmer's Technical Reference for the TITAN TTCN-3 Test Executor

[4] User Guide for the TITAN TTCN-3 Test Executor