IKEv2 protocol module for TTCN-3 Toolset with TITAN, Function Description

Eszter Susánszky

Version 1551-CNL 113 801, Rev. A, 2014-06-26

Table of Contents

How to Read This Document

This is the Function Specification for the set of IKEv2 protocol module. IKEv2 protocol module is developed for the TTCN-3 Toolset with TITAN.

Scope

The purpose of this document is to specify the content of the IKEv2 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 IKEv2 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 IKEv2 protocol. The module is based on RFC 4306). The following messages are

implemented:

- IKEv2_Message
- IKEv2_Header
- Payload_Header
- IKEv2_Payload
- Security_Association_Payload
- Key_Exchange_Payload
- Identification_Payload
- Certificate_Payload
- Certificate_Request_Payload
- Authentication_Payload
- Nonce_Payload
- Notify_Payload
- Delete_Payload
- Vendor_ID_Payload
- Traffic_Selector_Payload
- Encrypted_Payload
- Configuration_Payload
- EAP_Payload

Implemented Encoding/Decoding Functions:

Name	Type of formal parameters
ef_IKEv2_encode	in IKEv2_Message pl_pdu, in boolean pl_set_payload_type, out octetstring pl_stream
ef_IKEv2_decode	in octetstring pl_stream, out IKEv2_Message pl_pdu return integer
ef_IKEv2_Payloads_encode	in IKEv2_Payload pl_payloads, return octetstring pl_stream
ef_IKEv2_Payloads_decode	in octetsring pl_stream, in Next_Payload_Type pl _type, out IKEv2_Payloads pl_payload_list return integer

Terminology

No specific terminology is used.

Abbreviations

IKEv2

Internet Key Exchange Protocol

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 4306
IKEv2 Protocol Specification

[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