PPP Protocol Modules for TTCN-3 Toolset with TITAN, Function Specification

János Kövesdi

Version 155 17-CNL 113 599, Rev. B, 2013-09-02

Table of Contents

How to Read This Document

This is the Function Specification for the set of PPP protocol modules. PPP protocol modules are developed for the TTCN-3 Toolset with TITAN.

Scope

The purpose of this document is to specify the content of the PPP protocol modules.

General

Protocol modules implement the message structures of the related protocol in a formalized way, using the standard specification language TTCN-3. This allows defining of test data (templates) in the TTCN-3 language and correctly encoding/decoding messages when executing test suites using the TITAN TTCN-3 test environment.

Protocol modules are using TITAN's RAW encoding attributes [1] and hence are usable with the TITAN test toolset only.

Functional Specification

Protocol Version Implemented

This protocol module contains the protocol messages and elements of PPP [3] and its associated protocols IP [4], IPCP [4], PPP Extensions for Name Server Address [5], CHAP [6], PAP [7], EAP [9]-[11] and the `Address` and `Control` fields are defined in [8].

Modifications/Deviations Related to the Protocol Specification

Implemented Messages

All message types listed in protocol descriptions are implemented.

Protocol Modifications/Deviations

None.

Encoding/Decoding and Other Related Functions

This product also contains encoding/decoding functions that provide for the 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	Type of return value
enc_PDU_PPP	PDU_PPP	octetstring
dec_PDU_PPP	octetstring	PDU_PPP

NOTE The Address and Control fields defined in [9] are treated as a single optional field in the beginning of PDU_PPP.

Implemented PPP EAP functions (useful in RADIUS Protocol Module Generator):

Name	Type of parameters	Type of return value
f_enc_PDU_EAP	PDU_EAP	octetstring
f_dec_PDU_EAP	octetstring	PDU_EAP
f_enc_PDU_EAP_list	PDU_EAP_list	octetstring
f_dec_PDU_EAP_list	octetstring	PDU_EAP_list
f_enc_eap_sim_attrib_list	eap_sim_attrib_list	octetstring
f_dec_eap_sim_attrib_list	octetstring	eap_sim_attrib_list
f_enc_eap_aka_attrib_list	eap_aka_attrib_list	octetstring
f_dec_eap_aka_attrib_list	octetstring	eap_aka_attrib_list
f_calc_HMAC	octetstring, octetstring, integer	octetstring
f_initEAPPortDescriptor	EAP_port_descriptor (inout)	
f_get_EAP_parameters	octetstring (inout), EAP_port_descriptor (inout), Boolean	
f_set_Ki	integer, octetstring, EAP_port_descriptor (inout)	
f_set_K	integer, octetstring, EAP_port_descriptor (inout)	
f_set_SQN	integer, octetstring, EAP_port_descriptor (inout)	
f_set_SQN_MS	integer, octetstring, EAP_port_descriptor (inout)	
f_set_AMF	integer, octetstring, EAP_port_descriptor (inout)	

Name	Type of parameters	Type of return value
f_calc_AKA_Keys	octetstring, octetstring, octetstring octetstring, octetstring (inout), octetstring (inout), octetstring (inout)	octetstring
f_calc_A3A8	octetstring, octetstring	octetstring
f_calc_SRES	octetstring, octetstring	octetstring
f_calc_Kaut	octetstring, octetstring	octetstring
f_encrypt_at_encr	octetstring, octetstring octetstring, boolean	octetstring
f_crypt_atSimEncrData	at_sim_encr_data octetstring, octetstring, boolean	at_sim_encr_data
f_crypt_atAKAEncrData	at_aka_encr_data octetstring, octetstring, boolean	at_aka_encr_data

Terminology

TITAN TTCN-3 Test Executor.

Abbreviations

CHAP

PPP Challenge Handshake Authentication Protocol

IETF

Internet Engineering Task Force

IP

Internet Protocol

IPCP

PPP Internet Protocol Control Protocol

PAP

PPP Authentication Protocols

PPP

Point-to-Point Protocol

EAP

Extensible Authentication Protocol

RFC

Request for Comments

TTCN-3

Testing and Test Control Notation version 3

References

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

[2] ETSI ES 201 873-1 v.3.2.1 (2007-02)
The Testing and Test Control Notation version 3. Part 1: Core Language

[3] IETF RFC 1661
The Point-to-Point Protocol

[4] IETF RFC 1332
The PPP Internet Protocol Control Protocol (IPCP)

[5] IETF RFC 1877
PPP Internet Protocol Control Protocol Extensions for Name Server Address

[6] IETF RFC 1994
PPP Challenge Handshake Authentication Protocol (CHAP)

[7] IETF RFC 1334
PPP Authentication Protocols

[8] IETF RFC 1662
PPP in HDLC-like Framing

[9] IETF RFC 3748
Extensible Authentication Protocol (EAP)

[10] Extensible Authentication Protocol Method for GSM Subscriber Identity Modules (EAP-SIM)
https://tools.ietf.org/html/draft-haverinen-pppext-eap-sim-16 (2004-12)

[11] Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)
https://tools.ietf.org/html/draft-arkko-pppext-eap-aka-15 (2004-12)