ETSI TS 102 593 V1.2.0 (2008-04)

Technical Specification

Methods for Testing and Specification (MTS);
Internet Protocol Testing (IPT);
IPv6 Security;
Conformance Test Suite Structure and
Test Purposes (TSS&TP)

Reference

RTS/MTS-IPT-010[2]-IPv6-SecTSS

Keywords

IP, IPv6, security, testing, TSS&TP, TTCN

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Methods for Testing and Specification (MTS).

1 Scope

The purpose of the present document is to provide Test Suite Structure and Test Purposes (TSS&TP) for conformance tests of the security IPv6 protocol based on the requirements defined in the IPv6 requirements catalogue (TS 102 558 [2]) and written according to the guidelines of TS 102 351 [1], ISO/IEC 9646-2 [4] and ETS 300 406 [5].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI TS 102 351: "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT); IPv6 Testing: Methodology and Framework".

[2] ETSI TS 102 558: "Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT): IPv6 Security; Requirements Catalogue".

[3] ISO/IEC 9646-1: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 1: General concepts".

[4] ISO/IEC 9646-2: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 2: Abstract Test Suite specification".

[5] ETSI ETS 300 406: "Methods for Testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

Not applicable.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

abstract test case: Refer to ISO/IEC 9646-1 [3].

Abstract Test Method (ATM): Refer to ISO/IEC 9646-1 [3].

Abstract Test Suite (ATS): Refer to ISO/IEC 9646-1 [3].

Implementation Under Test (IUT): Refer to ISO/IEC 9646-1 [3].

Lower Tester (LT): Refer to ISO/IEC 9646-1 [3].

Test Purpose (TP): Refer to ISO/IEC 9646-1 [3].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AH	Authentication Header
ATM	Abstract Test Method
ATS	Abstract Test Suite
ESP	Encapsulating Security Payload
ICV	Integrity Check Value
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPv6	Internet Protocol version 6
IUT	Implementation Under Test
LT	Lower Test
RC	Requirements Catalogue
RQ	Requirement
TP	Test Purpose
TSS	Test Suite Structure
UDP	User Datagram Protocol

4 Test Suite Structure (TSS)

Test Purposes have been written for IPv6 mobile nodes, correspondent nodes and home agents according to the Requirements (RQ) of the Requirements Catalogue (RC) in TS 102 558 [2]. Test purposes have been written for behaviours requested with "MUST" or "SHOULD", optional behaviour described with "MAY" or similar wording indicating an option has not been turned into test purposes.

The test purposes have been divided into three groups:

Group 1: Authentication Header (AH)

Group 2: Encapsulating Security Payload (ESP)

Group 3: Key Exchange (IKEv2) Protocol

The sub-grouping of these three groups follows the structure of the RC.

Group 1: Authentication Header (AH)

Group 2: Encapsulating Security Payload (ESP)

Group 3: Key Exchange (IKEv2) Protocol

Group 3.1 Exchange Message Structures

Group 3.2 IKE Header and Payload Formats

Group 3.2.1 Configuration payload

Group 3.2.2 IKE Error Types

Group 3.3 IKE Informational Exchanges

Group 3.4 IKE Protocol

Group 3.4.1 Authentication

Group 3.4.1.1 Extensible Authentication Methods

Group 3.4.2 Error Handling

Group 3.4.3 General Protocol Handling

Group 3.4.3.1 Address and Port Agility

Group 3.4.3.2 IP Compression (IPComp)

Group 3.4.3.3 Message Format

Group 3.4.3.4 Overlapping Requests

Group 3.4.3.5 Request Internal Address

Group 3.4.3.6 Retransmission Timers

Group 3.4.3.7 Version Compatibility

Group 3.4.4 Security Parameter Negotiation

Group 3.4.4.1 Algorithm Negotiation

Group 3.4.4.2 Cookies

Group 3.4.4.3 Rekeying

Group 3.4.4.4 Traffic Selector Negotiation

Annex A (normative): Test Purposes (TP)

The test purposes have been written in the formal notation TPlan as described in annex A of TS 102 351 [1]. This original textual output ASCII file (SEC.tplan) is contained in archive ts_102593v010102p0.zip which accompanies the present document. The raw text file has been converted to a table format in this annex to allow better readability.

The two formats shall be considered equivalent. In the event that there appears to be syntactical or semantic differences between the two then the textual TPlan representation takes precedence over the table format in this annex.

A.1 Authentication Header (AH)

Test Purpose			
Identifier:	**TP_SEC_2000_01**		
Summary:	Test of generating first unicast IPv6 packets with Authentication Header		
References:	RQ_002_2000, RQ_002_2006, RQ_002_2011, RQ_002_2013, RQ_002_2015, RQ_002_2017, RQ_002_2027, RQ_002_2032, RQ_002_2033, RQ_002_2034, RQ_002_2036		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_2000_01

```
with { IUT and destination_node established in an AH_security_association
     }
ensure that
     { when { IUT is requested to send first unicast IPv6Packet
                    containing Authentication_Header }
       then { IUT sends IPv6Packet
                    containing next_header_field of previous_header
                        set to 51
                and containing (Authentication_Header
                                    containing Security_Parameters_Index
                                        set to Security_Parameters_Index
                                               received from destination_node
                                               during SA_establishment
                                and containing sequence_number set to 1
                                and containing correctly calculated
                                              Integrity_Check_Value
                                              including necessary padding_bits) }
     }
```


Test Purpose			
Identifier:	**TP_SEC_2000_02**		
Summary:	Test of generating subsequent unicast IPv6 packets with Authentication Header		
References:	RQ_002_2000, RQ_002_2006, RQ_002_2011, RQ_002_2012, RQ_002_2015, RQ_002_2017, RQ_002_2027, RQ_002_2032, RQ_002_2033, RQ_002_2034, RQ_002_2036		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_2000_02

```
with { IUT and destination_node established in an AH_security_association
     }
ensure that
     { when { IUT is requested to send subsequent unicast IPv6Packet
                    containing Authentication_Header }
       then { IUT sends IPv6Packet
                    containing next_header_field of previous_header
                        set to 51
                and containing (Authentication_Header
                                    containing Security_Parameters_Index
                                        set to Security_Parameters_Index
                                               received from destination_node
                                               during SA_establishment
                                and containing sequence_number set to
                                   (sequence_number of previous IPv6Packet) plus 1
                                and containing correctly calculated
                                              Integrity_Check_Value
                                              including necessary padding_bits) }
     }
```

Test Purpose			
Identifier:	**TP_SEC_2000_03**		
Summary:	Test of generating first multicast IPv6 packets with Authentication Header		
References:	RQ_002_2000, RQ_002_2007, RQ_002_2011, RQ_002_2013, RQ_002_2015, RQ_002_2017, RQ_002_2027, RQ_002_2032, RQ_002_2033, RQ_002_2034, RQ_002_2036		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_2000_03

```
with { IUT established in a multicast_group AH_Security_Association
     }
ensure that
     { when { IUT is requested to send first multicast IPv6Packet
                  containing Authentication_Header }
       then { IUT sends IPv6Packet
                  containing next_header_field of previous_header
                      set to 51
              and containing (Authentication_Header
                                  containing Security_Parameters_Index
                                             assigned to multicast_group
                                                         Security_Association
                              and containing sequence_number set to 1
                              and containing correctly calculated
                                              Integrity_Check_Value
                                              including necessary padding_bits) }
     }
```

Test Purpose			
Identifier:	**TP_SEC_2000_04**		
Summary:	Test of generating subsequent multicast IPv6 packets with Authentication Header		
References:	RQ_002_2000, RQ_002_2007, RQ_002_2011, RQ_002_2012, RQ_002_2015, RQ_002_2017, RQ_002_2027, RQ_002_2032, RQ_002_2033, RQ_002_2034, RQ_002_2036		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_2000_04

```
with { IUT established in multicast_group AH_Security_Association
     }
ensure that
     { when { IUT is requested to send subsequent multicast IPv6Packet
                  containing Authentication_Header }
       then { IUT sends IPv6Packet
                  containing next_header_field of previous_header
                      set to 51
              and containing (Authentication_Header
                                  containing Security_Parameters_Index
                                      set to Security_Parameters_Index
                                             assigned to multicast_group
                                                         Security_Association
                              and containing sequence_number set to
                                 (sequence_number of previous IPv6Packet) plus 1
                              and containing correctly calculated
                                            Integrity_Check_Value
                                            including necessary padding_bits) }
     }
```


Test Purpose			
Identifier:	**TP_SEC_2009_01**		
Summary:	Test reaction on IPv6 packets for unknown SA		
References:	RQ_002_2009		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_2009_01

```
with { IUT established in AH_Security_Association
     }
ensure that
     { when { IUT receives IPv6Packet
                  containing (Authentication_Header
                                  containing Security_Parameters_Index
                                             unrelated to established
                                             Security_Association) }
       then { IUT discards IPv6Packet }
     }
```

Test Purpose			
Identifier:	**TP_SEC_2042_01**		
Summary:	Test reaction on IPv6 packets with AH header and fragmentation header		
References:	RQ_002_2042		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_2042_01

```
with { IUT and destination_node established in an AH_security_association
     }
ensure that
     { when { IUT receives IPv6Packet
                  containing Authentication_Header
              and containing (Fragment_Header
                              containing offset not set to 0) }
       then { IUT discards IPv6Packet }
     }
```

Test Purpose			
Identifier:	**TP_SEC_2046_01**		
Summary:	Test reaction on IPv6 packets with AH header when no SA exists		
References:	RQ_002_2046		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_2046_01

```
with { IUT and destination_node not established in an AH_Security_Association
     }
ensure that
     { when { IUT receives IPv6Packet
                  containing Authentication_Header }
       then { IUT discards IPv6Packet }
     }
```


Test Purpose			
Identifier:	**TP_SEC_2053_01**		
Summary:	Test reaction on IPv6 packets with AH header with incorrect sequence number		
References:	RQ_002_2053		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_2053_01

```
with {     IUT and destination_node established in an AH_security_association
       and IUT and destination_node 'having already exchanged
                                     at least one packet'
     }
ensure that
     { when { IUT receives IPv6Packet
                  containing (Authentication_Header
                              containing sequence_number
                                  set to sequence_number received
                                     in previous IPv6packet) }
       then { IUT discards IPv6Packet }
     }
```

Test Purpose			
Identifier:	**TP_SEC_2057_01**		
Summary:	Test reaction on IPv6 packets with AH header with correct ICV value		
References:	RQ_002_2057, RQ_002_2028		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_2057_01

```
with { IUT and destination_node established in an AH_security_association
     }
ensure that
     { when { IUT receives IPv6Packet
                  containing (Authentication_Header
                              containing Integrity_Check_Value
                              calculated from Security_Association_data
                                          and packet_contents) }
       then { IUT accepts IPv6Packet }
     }
```

Test Purpose			
Identifier:	**TP_SEC_2058_01**		
Summary:	Test reaction on IPv6 packets with AH header with incorrect ICV value		
References:	RQ_002_2058, RQ_002_2028		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_2058_01

```
with { IUT and destination_node established in an AH_security_association
     }
ensure that
     { when { IUT receives IPv6Packet
                  containing (Authentication_Header
                              containing Integrity_Check_Value
                              not calculated from Security_Association_data
                                          and packet_contents) }
       then { IUT discards IPv6Packet }
     }
```

A.2 Encapsulating Security Payload (ESP)

Test Purpose			
Identifier:	**TP_SEC_3030_01**		
Summary:	Test reaction on ESP dummy packet		
References:	RQ_002_3030		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_3030_01

```
with { IUT and destination_node established in an ESP_Security_Association
     }
ensure that
     { when { IUT receives IPv6Packet
                  containing (ESP_Header
                              containing next_header_field set to 59) }
       then { IUT discards IPv6Packet }
     }
```

Test Purpose			
Identifier:	**TP_SEC_3061_01**		
Summary:	Test reaction on IPv6 packets with ESP header when no SA exists		
References:	RQ_002_3061, RQ_002_3091		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_3061_01

```
with { IUT 'has not established ESP Security Association with destination Node'
     }
ensure that
     { when { IUT receives IPv6Packet
                  containing ESP_Header }
       then { IUT discards IPv6Packet }
     }
```

Test Purpose			
Identifier:	**TP_SEC_3068_01**		
Summary:	Test reaction on IPv6 packets with ESP header with correct ICV value		
References:	RQ_002_3068, RQ_002_3072		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_3068_01

```
with {     IUT and destination_node established in an ESP_Security_Association
       and IUT 'having enabled anti-replay service'
     }
ensure that
     { when { IUT receives IPv6Packet
                  containing (ESP_Header
                              containing sequence_number
                              set to sequence_number from received IPv6Packet) }
       then { IUT discards IPv6Packet }
     }
```

Test Purpose			
Identifier:	**TP_SEC_3077_01**		
Summary:	Test reaction on IPv6 packets with ESP header with correct ICV value		
References:	RQ_002_3077		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_3077_01

```
with { IUT and destination_node established in an ESP_Security_Association
       and ESP_Security_Association configured to use
           combined_confidentiality_and_integrity_algorithms
     }
ensure that
     { when { IUT receives IPv6Packet
              containing (ESP_Header
                          containing Integrity_Check_Value
                          calculated from Security_Association_data
                                          and packet_contents) }
       then { IUT accepts IPv6Packet }
     }
```

Test Purpose			
Identifier:	**TP_SEC_3078_01**		
Summary:	Test reaction on IPv6 packets with ESP header with incorrect ICV value		
References:	RQ_002_3078, RQ_002_3077		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_3078_01

```
with { IUT and destination_node established in an ESP_Security_Association
       and ESP_Security_Association configured to use
           combined_confidentiality_and_integrity_algorithms
     }
ensure that
     { when { IUT receives IPv6Packet
              containing (ESP_Header
                          containing Integrity_Check_Value
                          not calculated from Security_Association_data
                                          and packet_contents) }
       then { IUT discards IPv6Packet }
     }
```

Test Purpose			
Identifier:	**TP_SEC_3080_01**		
Summary:	Test reaction on IPv6 packets with ESP header with correct ICV value		
References:	RQ_002_3080		
IUT Role:	Ipsec_host	**Test Case:**	TC_SEC_3080_01

```
with { IUT and destination_node established in an ESP_Security_Association
       and ESP_Security_Association configured to use
           separate_confidentiality_and_integrity_algorithms
     }
ensure that
     { when { IUT receives IPv6Packet
              containing (ESP_Header
                          containing Integrity_Check_Value
                          calculated from Security_Association_data
                                          and packet_contents) }
       then { IUT accepts IPv6Packet }
     }
```