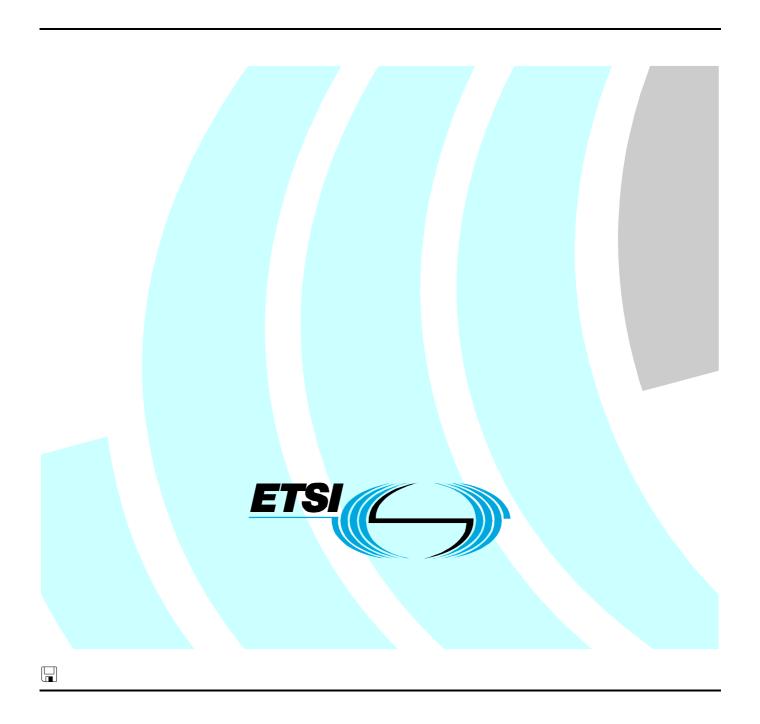
ETSITS 102 593 V1.2.0 (2008-04)

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: <u>http://www.etsi.org</u>

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

No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2008. All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM, **TIPHON**TM, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP[™] is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intelle	lectual Property Rights	
Forew	word	4
1	Scope	5
2	References	4
2.1	Normative references	
2.1	Informative references	
3	Definitions and abbreviations	
3.1	Definitions	
3.2	Abbreviations	6
4	Test Suite Structure (TSS)	<i>.</i>
Anne	ex A (normative): Test Purposes (TP)	
A.1	Authentication Header (AH)	3
A.2	Encapsulating Security Payload (ESP)	11
A.3	Key Exchange (IKEv2) Protocol	17
A.3.1	•	
A.3.2		
A.3.2.	2.1 Configuration payload	
A.3.2.2	2.2 IKE Error Types	23
A.3.3	<u> </u>	
A.3.4		
A.3.4.		
A.3.4.		
A.3.4.2		
A.3.4.3	\mathcal{E}	
A.3.4.3		
A.3.4.3	1 ' 1'	
A.3.4.	E .	
A.3.4.	11 0 1	
A.3.4.	1	
A.3.4.3		
A.3.4.3	1 3	
A.3.4.4		
A.3.4.4	6 · · · · · · · · · · · · · · · · · · ·	
A.3.4.4		
A.3.4.4	, <i>e</i>	
A.3.4.4	C	
Anne	ex B (informative): Bibliography	45
Tictor	OW.	14

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 ExchangeIPv6 Internet Protocol version 6IUT 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				
ensure that	estination_node established in an AH_security_association				
{ when { IUT is requested to send first unicast IPv6Packet					
}	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) }				

	Tot Downson						
	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:	lpsec_host Test Case: TC_SEC_2000_02						
with { IUT and de	estination_node established in an AH_security_association						
}							
ensure that							
{ when { IU	I is requested to send subsequent unicast IPv6Packet						
,	<pre>containing Authentication_Header }</pre>						
then { IU	F sends IPv6Packet						
	<pre>containing next_header_field of previous_header</pre>						
	set to 51						
and	d containing (Authentication_Header						
	<pre>containing Security_Parameters_Index</pre>						
	<pre>set to Security_Parameters_Index</pre>						
	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						
	<pre>including necessary padding bits) }</pre>						
}							

```
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:
                  lpsec_host
                                                Test Case:
                                                                              TC_SEC_2000_03
with { IUT established in a multicast group AH Security Association
ensure that
     \{\mbox{ when }\{\mbox{ IUT is requested to send first }\mbox{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:	lpsec_host Test Case: TC_SEC_2000_04						
with { IUT establ	.ished in multicast_group AH_Security_Association						
}							
ensure that { when { IUT	lis namental to and subsequent multiment TDecDerlet						
{ wnen { 101	is requested to send subsequent multicast IPv6Packet containing Authentication Header }						
then { TIT	sends IPv6Packet						
Chen (101	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						
	<pre>including necessary padding_bits) }</pre>						
}							

	-	Test Purpose	
Identifier:	TP_SEC_2009_01		
Summary:	Test reaction on IPv6 packets for	unknown SA	
References:	RQ_002_2009		
IUT Role:	lpsec_host	Test Case:	TC_SEC_2009_01
ensure that { when { IUI	unre		

```
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:
                                              Test Case:
                                                                            TC_SEC_2042_01
                 lpsec_host
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 r	no SA exists				
References:	RQ_002_2046						
IUT Role:	lpsec_host	Test Case:	TC_SEC_2046_01				
ensure that { when { IUI	receives IPv6Packet containing Authentication_He discards IPv6Packet }	_	rity_Association				

		Test Purpose	
Identifier:	TP_SEC_2053_01		
Summary:	Test reaction on IPv6	packets with AH header with incor	rect sequence number
References:	RQ_002_2053		
IUT Role:	lpsec_host	Test Case:	TC_SEC_2053_01
with { IUT ar	nd destination_node	e established in an AH_securit	y_association
and IUT ar	nd destination_node	'having already exchanged	
		at least one packet'	
}			
ensure that			
{ when { IUT	receives IPv6Pack	cet	
	containing (Authe	entication_Header	
	conta	ining sequence number	
	s	set to sequence number receive	ed
		<pre>in previous IPv6packet) }</pre>	
then { IUT	discards IPv6Pack	cet }	
}			

```
Test Purpose
Identifier:
                 TP_SEC_2057_01
                 Test reaction on IPv6 packets with AH header with correct ICV value
Summary:
References:
                 RQ_002_2057, RQ_002_2028
                                              Test Case:
                                                                            TC_SEC_2057_01
IUT Role:
                 Ipsec_host
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
                                                                            TC_SEC_2058_01
IUT Role:
                 lpsec_host
                                               Test Case:
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:
                                             Test Case:
                                                                           TC_SEC_3030_01
                Ipsec_host
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	n ESP header when no	o SA exists				
References:	RQ_002_3061, RQ_002_3091						
IUT Role:	lpsec_host	Test Case:	TC_SEC_3061_01				
ensure that { when { IUI	receives IPv6Packet containing ESP_Header } discards IPv6Packet }	Association with d	estination Node'				

```
Test Purpose
Identifier:
                 TP SEC 3068 01
Summary:
                 Test reaction on IPv6 packets with ESP header with correct ICV value
                 RQ_002_3068, RQ_002_3072
References:
IUT Role:
                 lpsec_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
                   TP_SEC_3077_01
Identifier:
                   Test reaction on IPv6 packets with ESP header with correct ICV value
Summary:
References:
                   RQ_002_3077
IUT Role:
                                                  Test Case:
                                                                                  TC_SEC_3077_01
                  Ipsec_host
       IUT and destination_node established in an ESP_Security_Association and ESP_Security_Association configured to use
with {
                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 p	packets with ESP header with incor	rect ICV value
References:	RQ_002_3078, RQ_00	02_3077	
IUT Role:	lpsec_host	Test Case:	TC_SEC_3078_01
and ESP_Se CC } ensure that { when { IU	ecurity_Association ombined_confidential I receives IPv6Packe containing (ESP_He contai	<pre>ity_and_integrity_algorithms t ader ning Integrity_Check_Value lculated from Security_Associ</pre>	

		Test Purpose	
Identifier:	TP_SEC_3080_01		
Summary:	Test reaction on IPv6 pa	ackets with ESP header with cor	rect ICV value
References:	RQ_002_3080		
IUT Role:	lpsec_host	Test Case:	TC_SEC_3080_01
and ESP_Se se } ensure that { when { IU	ecurity_Association c eparate_confidentiali Treceives IPv6Packet containing (ESP_Hea contain	der integrity_Algorithms der ing Integrity_Check_Value ted from Security_Associate and packet_contents)	ion_data

```
Test Purpose
                  TP_SEC_3083_01
Identifier:
                   Test reaction on IPv6 packets with ESP header with incorrect ICV value
Summary:
References:
                  RQ_002_3083, RQ_002_3080
IUT Role:
                                                 Test Case:
                                                                                TC_SEC_3083_01
                  Ipsec_host
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
not calculated from Security_Association_data
                                             and packet_contents) }
       then { IUT discards IPv6Packet }
```

			Test Purpose				
Identifier:	TP_SEC_3102_01						
Summary:	Test of generating fi	rst unicast IP	v6 packets with E	SP Header, trans	port mode		
References:	RQ_002_3102, RQ RQ_002_3037, RQ		RQ_002_3005,	RQ_002_3009,	RQ_002_3012,	RQ_002_3027,	
IUT Role:	lpsec_host		Test Case:		TC_SEC_3102_	01	
	d destination_nod			ecurity_Associa	ation		
	curity_Association						
se	parate_confidenti	lality_and_i	.ntegrity_algor	ithms			
}							
ensure that			TDCDlt d				
{ when { 101	is requested to containing ESP F		ipvopacket in	transport_mode			
then { IUT	sends IPv6Packet		ort mode				
chen / 101	containing next	_	_	header			
	set to 50	_neader_rrer	d Or previous_	neader			
and	containing (ESP	Header					
		_	rity Parameter	s Index			
		set to Secu	rity Parameter	s Index			
		rece	ived from dest	ination_node			
		duri	.ng SA_establis	hment			
			ence_number se				
			ssary padding_	bytes			
	<pre>and containing pad_length</pre>						
	set to number of padding_bytes						
	and containing correctly calculated						
	<pre>Integrity_Check_Value including necessary padding bits) }</pre>						
1	inci	rading neces	pary badding_p	TCD) }			
}							

```
Test Purpose
Identifier:
                 TP SEC 3102 02
Summary:
                 Test of generating subsequent unicast IPv6 packets with ESP Header, transport mode
References:
                 RQ 002 3102, RQ 002 3004, RQ 002 3005, RQ 002 3006, RQ 002 3009, RQ 002 3027,
                 RQ_002_3037, RQ_002_3112
IUT Role:
                                             Test Case:
                                                                          TC_SEC_3102_02
                 lpsec_host
           IUT and destination_node established in an ESP_Security_Association
with {
       and ESP Security Association configured to use
               separate_confidentiality_and_integrity_algorithms
ensure that
     { when { IUT is requested to send subsequent IPv6Packet in transport mode
                  containing ESP Header }
       then { IUT sends IPv6Packet in transport_mode
                  containing next_header_field of previous_header
                      set to 50
              and containing (ESP 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 necessary padding_bytes
                          and containing pad length
                                  set to number of padding_bytes
                          and containing correctly calculated
                                        Integrity_Check_Value
                              including necessary padding bits) }
```

		Test Purpose					
Identifier: TP_SEC_3103_01							
Summary:	Test of generating fi	rst unicast IPv6 packets with E	SP Header, tunne	el mode			
References:		Q_002_3004, RQ_002_3005, _002_3092, RQ_002_3113	RQ_002_3009,	RQ_002_3012,	RQ_002_3027,		
IUT Role:	Ipsec_host	Test Case:		TC_SEC_3103_	01		
	nd destination_nod	le established in an ESP_S	ecurity_Associa				
and ESP_Se	ecurity_Associatio	on configured to use					
Se	eparate_confidenti	.ality_and_integrity_algor	ithms				
}							
ensure that							
{ when { IU	-	send first IPv6Packet in	tunnel_mode				
*b (TIT	containing ESP_H						
then { IU	r sends IPv6Packet	_					
	set to 50	_header_field of previous_	neader				
and	d containing (ESP	Header					
	_	caining Security Parameter	s Index				
	00110	set to Security_Parameter					
		received from dest					
		during SA establis	hment				
	and cont	aining sequence number se	t to 1				
	and cont	aining necessary padding_	bytes				
	and containing pad_length						
	set to number of padding_bytes						
	and containing correctly calculated						
	Integrity_Check_Value						
	incl	.uding necessary padding_b	its) }				
}							

```
Test Purpose
Identifier:
                 TP SEC 3103 02
Summary:
                 Test of generating subsequent unicast IPv6 packets with ESP Header, tunnel mode
References:
                 RQ_002_3103, RQ_002_3004, RQ_002_3005, RQ_002_3006, RQ_002_3009, RQ_002_3027,
                 RQ_002_3037, RQ_002_3092, RQ_002_3112
                                             Test Case:
IUT Role:
                                                                          TC_SEC_3103_02
                lpsec_host
           IUT and destination_node established in an ESP_Security_Association
with {
       and ESP Security Association configured to use
               separate_confidentiality_and_integrity_algorithms
ensure that
     { when { IUT is requested to send subsequent IPv6Packet in tunnel mode
                  containing ESP Header }
       then { IUT sends IPv6Packet in tunnel_mode
                  containing next_header_field of previous_header
                      set to 50
              and containing (ESP 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 necessary padding_bytes
                          and containing pad length
                                  set to number of padding_bytes
                          and containing correctly calculated
                                        Integrity_Check_Value
                              including necessary padding bits) }
```

		Test Purpose	
Identifier:	TP_SEC_3107_01		
Summary:	Test of generating first unicast	IPv6 packets with ESP Header, trans	sport mode
References:	RQ 002 3102, RQ 002 300	4, RQ 002 3005, RQ 002 3009,	RQ 002 3012, RQ 002 3027,
	RQ_002_3113	. – – . – – .	
IUT Role:	lpsec_host	Test Case:	TC_SEC_3107_01
with { IUT ar	nd destination_node establi	shed in an ESP_Security_Associ	ation
and ESP_Se	ecurity_Association configu	red to use	
CC	ombined_confidentiality_and	_integrity_algorithms	
}			
ensure that			
{ when { IUT		<pre>t IPv6Packet in transport_mode</pre>	
	containing ESP_Header }	_	
then { IUT	r sends IPv6Packet in trans		
	containing next_header_fi	eld of previous_header	
	set to 50		
and	d containing (ESP_Header	and the December To do	
		curity_Parameters_Index	
		curity_Parameters_Index ceived from destination node	
		ring SA establishment	
		quence number set to 1	
		cessary padding bytes	
	and containing ne		
		mber of padding bytes	
		rrectly calculated	
		egrity Check Value	
		essary padding bits) }	
}	3	<u> </u>	
}			

```
Test Purpose
Identifier:
                 TP SEC 3107 02
Summary:
                 Test of generating subsequent unicast IPv6 packets with ESP Header, transport mode
References:
                 RQ 002 3107, RQ 002 3004, RQ 002 3005, RQ 002 3006, RQ 002 3009, RQ 002 3027,
                 RQ_002_3112
                Ipsec_host
IUT Role:
                                             Test Case:
                                                                          TC_SEC_3107_02
           IUT and destination_node established in an ESP_Security_Association
with {
       and ESP Security Association configured to use
               combined_confidentiality_and_integrity_algorithms
ensure that
     { when { IUT is requested to send subsequent IPv6Packet in transport mode
                  containing ESP Header }
       then { IUT sends IPv6Packet in transport_mode
                  containing next_header_field of previous_header
                      set to 50
              and containing (ESP 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 necessary padding_bytes
                          and containing pad length
                                  set to number of padding_bytes
                          and containing correctly calculated
                                        Integrity_Check_Value
                              including necessary padding_bits) }
```

	Test Purpose		
Identifier:	TP_SEC_3108_01		
Summary:	est of generating first unicast IPv6 packets with ESP Header, tunnel mode		
References:	RQ_002_3108, RQ_002_3004, RQ_002_3005, RQ_002_3009, RQ_002_3012, RQ_002_3027, RQ_002_3092, RQ_002_3113		
IUT Role:	lpsec_host Test Case: TC_SEC_3108_01		
and ESP_Se cc } ensure that { when { IUT then { IUT	d destination_node established in an ESP_Security_Association courity_Association configured to use published_confidentiality_and_integrity_algorithms T is requested to send first IPv6Packet in tunnel_mode containing ESP_Header } T sends IPv6Packet in tunnel_mode containing next_header_field of previous_header set to 50 I containing (ESP_Header		

```
Test Purpose
Identifier:
                 TP SEC 3108 02
                 Test of generating subsequent unicast IPv6 packets with ESP Header, tunnel mode
Summary:
References:
                 RQ 002 3108, RQ 002 3004, RQ 002 3005, RQ 002 3006, RQ 002 3009, RQ 002 3027,
                 RQ_002_3092, RQ_002_3112
                                              Test Case:
IUT Role:
                                                                            TC_SEC_3108_02
                 Ipsec_host
with {
           IUT and destination node established in an ESP Security Association
       and ESP Security Association configured to use
               {\tt combined\_confidentiality\_and\_integrity\_algorithms}
ensure that
     { when { IUT is requested to send subsequent IPv6Packet in tunnel mode
                  containing ESP Header }
       then { IUT sends IPv6Packet in tunnel_mode
                  containing next_header_field of previous_header
                      set to 50
              and containing (ESP 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 necessary padding_bytes
                          and containing pad length
                                  set to number of padding bytes
                          and containing correctly calculated
                                         Integrity_Check_Value
                               including necessary padding bits) }
```

A.3 Key Exchange (IKEv2) Protocol

A.3.1 Exchange Message Structures

```
Test Purpose
                 TP_SEC_6400_01
Identifier:
Summary:
                 Test of generating IKE_SA_INIT request
References:
                 RQ_002_6400, RQ_002_6034, RQ_002_6077, RQ_002_6084, RQ_002_6085, RQ_002_6086,
                 RQ_002_6128, RQ_002_6129, RQ_002_6232, RQ_002_6236, RQ_002_6240, RQ_002_6250,
                 RQ_002_6263, RQ_002_6304, RQ_002_6344
IUT Role:
                                                                           TC_SEC_6400_01
                 Host
                                              Test Case:
with { IUT ready to establish a Security_Association using IKEv2
ensure that
     { when { IUT is requested to send IKE_SA_INIT_request }
       then { IUT sends IKE_SA_INIT_request
                  {\tt containing} \ ({\tt IKE\_Header}
                              containing IKE_SA_Initiators_SPI not set to 0
                          and containing IKE_SA_Responders_SPI set to 0
                          and containing Major Version set to 2
                          and containing Exchange_Type set to 34 IKE_SA_INIT
                          and containing Flags set to 00010000'B'
                          and containing Message_ID set to 0)
              and containing (Security Association payload
                              containing at least 1 Proposal
                                         containing at least 1 Transform)
              and containing Key_Exchange_payload
              and containing (Nonce_payload
                              containing Nonce Data
                                     of at least 128 bits
                                     and 'at least half the prf key length') }
```

```
Test Purpose
Identifier:
                  TP_SEC_6401_01
Summary:
                  Test reaction on IKE_SA_INIT request
References:
                  RQ 002 6401, RQ 002 6036, RQ 002 6232, RQ 002 6233, RQ 002 6236, RQ 002 6240,
                  RQ_002_6250, RQ_002_6263, RQ_002_6304, RQ_002_6344
                                                 Test Case:
IUT Role:
                  Host
                                                                                TC_SEC_6401_01
with { IUT ready to establish Security Association using IKEv2
ensure that
     { when { IUT receives IKE_SA_INIT_request }
  then { IUT sends IKE_SA_INIT_response
                   containing (IKE_Header
                                containing IKE_SA_Initiators_SPI
                                    set to IKE_SA_Initiators_SPI
                                           received in IKE_SA_INIT_request
                            and containing IKE SA Responders SPI not set to 0
                            and containing Major_Version set to 2
and containing Exchange_Type set to 34 IKE_SA_INIT
                            and containing Flags set to 00000100'B'
                            and containing Message_ID
                                    set to Message_ID
                                            received in IKE_SA_INIT_request)
               and containing (Security_Association_payload
                                containing 1 proposal
                                            received in IKE_SA_INIT_request)
               and containing Key_Exchange_payload
               and containing Nonce_payload }
```

			Test Purpose			
Identifier:	TP SEC 6403		reat Furpose			
Summary:		Test of generating IKE_AUTH request				
References:	RQ_002_6403, RQ_002_6034, RQ_002_6084, RQ_002_6085, RQ_002_6086, RQ_002_623				RO 002 6232	
ixelelelices.				RQ_002_6250,		
	RQ_002_6233,		NQ_002_0240,	NQ_002_0250,	NQ_002_0203,	NQ_002_0310,
IIIT Dala:		KQ_002_0431	Tool Cook		TO 050 0400	04
IUT Role:	Host	G3 T31TM	Test Case:		TC_SEC_6403_	.01
		_SA_INIT_reques _IKE_SA_INIT_re				
		to send IKE_AU	TH_request }			
then { IU	r sends IKE_AU'					
	containing (
	(containing IKE_				
			SA_Initiators_			
	•		ived in IKE_SA			
	and o	containing IKE_				
		_	SA_Responders_	INIT response		
	and a	rece containing Majo				
		containing Majo				
		containing Exem				
		containing Mess				
and containing (Encrypted payload						
		containing Iden		load initiator		
			Payload field			
		payl	oad is set to	35'		
	and o	containing Auth	entication_pay	load		
	and o	containing(Secu	rity_Associati	on_payload		
		cont	aining at leas	t 1 proposal		
				least 1 trans	· ·	
	and o			ayload_initiato	or	
			Payload field	-		
			oad is set to			
	and o			ayload_responde	er	
			Payload field			
,		payl	oad is set to	45') }		
}						

```
Test Purpose
Identifier:
                 TP SEC 6405 01
Summary:
                 Test reaction on IKE_AUTH request
References:
                 RQ 002 6405, RQ 002 6036, RQ 002 6232, RQ 002 6233, RQ 002 6236, RQ 002 6240,
                 RQ_002_6250, RQ_002_6263, RQ_002_6312, RQ_002_6430, RQ_002_6431
                                                                            TC_SEC_6405_01
IUT Role:
                 Host
                                              Test Case:
          IUT having received IKE SA INIT request
with {
      and IUT having sent IKE SA INIT response
ensure that
     { when { IUT receives IKE_AUTH_request }
  then { IUT sends IKE_AUTH_response
                  containing (IKE Header
                               containing IKE_SA_Initiators_SPI
                                   set to IKE_SA_Initiators_SPI
                                         received in IKE SA INIT request
                          and containing IKE SA Responders SPI
                                   set to IKE SA Responders SPI
                                          sent in IKE SA INIT response
                          and containing Major_Version set to 2
                          and containing Exchange_Type set to 35 IKE_AUTH
                          and containing Flags set to 00000100'B'
                          and containing Message_ID
                                   set to Message_ID
                                          received in IKE AUTH request)
              and containing (Encrypted payload
                               containing Identification_payload_responder
                                         'Next Payload field of previous payload
                                          is set to 36'
                          and containing Authentication payload
                          and containing (Security Association payload
                                           containing 1 proposal
                                                 received in IKE_AUTH_request)
                          and containing Traffic_Selector_payload_initiator
                                         'Next Payload field of previous payload
                                          is set to 44'
                          and containing Traffic_Selector_payload_responder
                                         'Next Payload field of previous payload
                                          is set to 45' }
```

```
Test Purpose
Identifier:
                  TP SEC 6407 01
Summary:
                  Test of generating CREATE_CHILD_SA request
References:
                  RQ_002_6407, RQ_002_6035, RQ_002_6084, RQ_002_6085, RQ_002_6086, RQ_002_6128,
                  RQ_002_6129, RQ_002_6232, RQ_002_6233, RQ_002_6236, RQ_002_6240, RQ_002_6250,
                  RQ_002_6263, RQ_002_6344
IUT Role:
                                                Test Case:
                                                                              TC_SEC_6407_01
                  Host
           IUT having completed IKE_SA INIT exchange
with {
       and IUT having completed IKE AUTH exchange
ensure that
       when { IUT is requested to send CREATE_CHILD_SA_request }
then { IUT sends CREATE_CHILD_SA_request
                   containing (IKE Header
                               containing IKE_SA_Initiators_SPI
set to IKE_SA_Initiators_SPI
                                      sent or received in the IKE_SA_INIT_request
                           and containing IKE SA Responders SPI
                                   set to IKE SA Responders SPI
                                      sent or received in the IKE_SA_INIT_response
                           and containing Major_Version set to 2
                           and containing Exchange_Type set to 36 CREATE_CHILD_SA
                           and containing Flags set to 00010000'B'
                           and containing Message ID
                                   set to previous sent Message_ID plus 1)
              and containing (Encrypted_payload
                               containing (Security_Association_payload
                                            containing at least 1 proposal
                                                  containing at least 1 transform)
                           and containing (Nonce_payload
                                            containing Nonce Data
                                                       of at least 128 bits
                                                     and 'at least half the
                                                          prf key length')
                           and containing Traffic_Selector_payload_initiator
                                          'Next Payload field of previous
                                           payload is set to 44'
                           and containing Traffic_Selector_payload_responder
                                          'Next Payload field of previous
                                           payload is set to 45')}
```

```
Test Purpose
Identifier:
                 TP SEC 6409 01
Summary:
                 Test reaction on CREATE_CHILD_SA request
                 RQ 002 6409, RQ 002 6036, RQ 002 6232, RQ 002 6233, RQ 002 6236, RQ 002 6240,
References:
                 RQ_002_6250, RQ_002_6263, RQ_002_6344
                                               Test Case:
IUT Role:
                                                                            TC_SEC_6409_01
                 Host
           IUT having completed IKE SA INIT exchange
with {
       and IUT having completed IKE AUTH exchange
ensure that
     { when { IUT receives CREATE_CHILD_SA_request }
  then { IUT sends CREATE_CHILD_SA_response
                  containing (IKE Header
                               containing IKE_SA_Initiators_SPI
                                   set to IKE SA Initiators SPI
                                   sent or received in the IKE SA INIT request
                           and containing IKE SA Responders SPI
                                   set to IKE SA Responders SPI
                                   sent or received in the IKE SA INIT request
                           and containing Major_Version set to 2
                           and containing Exchange_Type set to 36 CREATE_CHILD_SA
                           and containing Flags set to 00000100'B'
                           and containing Message_ID
                                   set to Message_ID
                                          received in CREATE CHILD SA request)
              and containing (Encrypted payload
                               containing (Security_Association_payload
                                           containing 1 proposal
                                             received in CREATE CHILD SA request)
                           and containing Nonce payload
                           and containing Traffic Selector payload initiator
                                          'Next Payload field of previous
                                          payload is set to 44'
                           and containing Traffic_Selector_payload_responder
                                          'Next Payload field of previous
                                          payload is set to 45')}
```

		Test Purpose			
Identifier:	TP_SEC_6411_01	-			
Summary:	Test of generating INFORMATION	NAL_request			
References:	RQ_002_6411, RQ_002_6035, RQ_002_6250	RQ_002_6232, RQ_002_6233,	RQ_002_6236, RQ_002_6240,		
IUT Role:	Host	Test Case:	TC_SEC_6411_01		
ensure that { when { IUT	g established an IKE_Security T is requested to send INFORM T sends INFORMATIONAL_request containing (IKE_Header	_ ATIONAL_request }			
		SA_Initiators_SPI			
		SA_Initiators_SPI			
	sent or received in the IKE_SA_INIT_request				
	<pre>and containing IKE_SA_Responders_SPI set to IKE SA Responders SPI</pre>				
	set to IKE_SA_Responders_SPI sent or received in the IKE_SA_INIT_request				
	and containing Majo		ies c		
		ange_Type set to 37 INFORMATI	IONAL		
		s set to 00010000'B'			
	and containing Mess				
and	d containing (Encrypted_paylo containing 0 or and containing 0 or	<pre>ious sent Message_ID plus 1) ad more Notify_payload more Delete_payload more Configuration payload)</pre>	3		
}			,		

```
Test Purpose
Identifier:
                 TP SEC 6412 01
                 Test reaction on INFORMATIONAL request
Summary:
                 RQ 002 6412, RQ 002 6036, RQ 002 6232, RQ 002 6233, RQ 002 6236, RQ 002 6240,
References:
                 RQ_002_6250
                                             Test Case:
IUT Role:
                                                                          TC_SEC_6412_01
                 Host
with {
      IUT having established an IKE Security Association
ensure that
      when
             IUT receives INFORMATIONAL_request }
       then { IUT sends INFORMATIONAL response
                  containing (IKE Header
                              containing IKE_SA_Initiators_SPI
                                  set to IKE SA Initiators SPI
                                  sent or received in the IKE SA INIT request
                          and containing IKE SA Responders SPI
                                  set to IKE SA Responders SPI
                                  sent or received in the IKE SA INIT request
                          and containing Major_Version set to 2
                          and containing Exchange_Type set to 37 INFORMATIONAL
                          and containing Flags set to 00000100'B'
                          and containing Message_ID
                                  set to Message_ID
                                         received in INFORMATIONAL_request)
              and containing (Encrypted payload
                              containing 0 or more Notify payload
                          and containing 0 or more Delete_payload
                          and containing 0 or more Configuration_payload) }
```

A.3.2 IKE Header and Payload Formats

A.3.2.1 Configuration payload

```
Test Purpose
Identifier:
                 TP_SEC_6468_01
Summary:
                 Test reaction on INFORMATIONAL_request with unsupported Configuration payload
References:
                 RQ_002_6468
                                                                            TC_SEC_6468_01
IUT Role:
                                              Test Case:
                 Host
with { IUT having established an IKE Security Association
ensure that
                 IUT receives INFORMATIONAL_request
     { when {
                     containing (Configuration payload
                                  containing Configuration_Type
                                      set to 1 CFG_REQUEST
                              and containing any unsupported
                                             Configuration_Attribute) }
                 IUT sends INFORMATIONAL_response
       then {
                     containing (Configuration_payload
                                  containing Configuration_Type
                                      set to 2 CFG REPLY
                         and not containing any unsupported
                                             Configuration Attribute)
              or not containing (Configuration_payload) }
```

A.3.2.2 IKE Error Types

		Test Purpose		
Identifier:	TP_SEC_6365_01	P_SEC_6365_01		
Summary:	Test reaction on INFORMATION	AL_request containing incor	rect value	
References:	RQ_002_6365, RQ_002_6368			
IUT Role:	Host	Test Case:	TC_SEC_6365_01	
ensure that { when { IUI	receives INFORMATIONAL requestion receives INFORMATIONAL requestion requestion of sends INFORMATIONAL response containing (Encrypted paylocontaining Notice)	uest incorrect value' } se pad		

		Test Purpose				
Identifier:	TP_SEC_6375_01					
Summary:	Test reaction on CRE	st reaction on CREATE_CHILD_SA request containing Traffic Selectors indicating address range				
References:	RQ_002_6375	· · · · · · · · · · · · · · · · · · ·				
IUT Role:	Host	Test Case:	TC_SEC_6375_01			
with { IUT ha	aving established a	n IKE_Security_Association				
and IUT 'c	only supporting Tra	ffic Selectors specifying a				
٤	single pair of addr	esses'				
}						
ensure that						
{ when { IU	receives CREATE_CHILD_SA_request					
	containing (Traff	containing (Traffic_Selector_payload				
	conta	ining Traffic Selector				
	i	<pre>ndicating 'address range') }</pre>				
then { IUT	hen { IUT sends CREATE_CHILD_SA_response					
	containing (Notif	y payload				
	conta	<pre>ining Notify_Message_Type</pre>				
	£	et to 34 SINGLE PAIR REQUIRED)	}			
}						

	Test Purpose			
Identifier:	P_SEC_6376_01			
Summary:	Test reaction on CREATE_CHILD_SA request when no	est reaction on CREATE_CHILD_SA request when no more CHILD_SA can be established		
References:	RQ_002_6376			
IUT Role:	Host Test Case:	TC_SEC_6376_01		
and IUT 'u } ensure that { when { IU	aving established an IKE_Security_Association unable to establish any further CHILD_SA' T receives CREATE_CHILD_SA_request } T sends CREATE_CHILD_SA_response	}		

```
Test Purpose
                TP_SEC_6379_01
Identifier:
                Test reaction on CREATE_CHILD_SA request containing unacceptable Traffic Selectors
Summary:
References:
               RQ_002_6379
IUT Role:
                                          Test Case:
                                                                    TC_SEC_6379_01
               Host
with { IUT having established an IKE_Security_Association
ensure that
    { when { IUT receives CREATE_CHILD_SA_request
                containing (Traffic_Selector_payload
                           containing 1 or more
                                     unacceptable Traffic_Selector) }
      then { IUT sends CREATE CHILD SA response
```

	7	Test Purpose		
Identifier:	TP_SEC_6393_01	P_SEC_6393_01		
Summary:	Test reaction on CREATE_CHILD	_SA request containing tr	ansport mode request	
References:	RQ_002_6393			
IUT Role:	Host	Test Case:	TC_SEC_6393_01	
	wing established an IKE_Secu			
ensure that { when { IUI	<pre>Sends CREATE_CHILD_SA_respon containing (Notify_payload containing Notify</pre>	quest Fy_Message_Type L USE_TRANSPORT_MODE) nse		

		Test Purpose			
dentifier:	TP_SEC_6394_01	-			
Summary:	Test reaction on CR	Test reaction on CREATE_CHILD_SA request containing transport mode request			
References:	RQ_002_6394	· -	·		
UT Role:	Host	Test Case:	TC_SEC_6394_01		
•	_	an IKE_Security_Association			
and IUT	'not ready to accep	t transport mode request'			
ensure that					
	IUT receives CREATE	CHILD SA remiest			
(when (containing (Noti				
		aining Notify Message Type			
		set to 16391 USE TRANSPORT MODE) }		
$ exttt{then}$ {	IUT sends CREATE_CHI	sends CREATE_CHILD_SA_response			
1	not containing (Noti	fy_payload			
	cont	aining Notify_Message_Type			
		set to 16391 USE_TRANSPORT_MODE) }		
}					

A.3.3 IKE Informational Exchanges

```
Test Purpose
Identifier:
                 TP_SEC_6007_01
Summary:
                 Test reaction on INFORMATIONAL_request without payload
References:
                 RQ_002_6007, RQ_002_6012
IUT Role:
                                                                           TC_SEC_6007_01
                                              Test Case:
                 Host
with { IUT having established an IKE_Security_Association
ensure that
     { when { IUT receives INFORMATIONAL_request
                  not containing a payload }
       then { IUT sends INFORMATIONAL_response }
```

```
Test Purpose
Identifier:
                 TP_SEC_6014_01
                 Test of generating INFORMATIONAL_request with Delete payload for IKE_SA
Summary:
References:
                 RQ_002_6014, RQ_002_6016, RQ_002_6062, RQ_002_6064, RQ_002_6415,RQ_002_6416,
                 RQ_002_6417
IUT Role:
                                                                          TC_SEC_6014_01
                                             Test Case:
                 Host
           IUT having established an IKE_Security_Association
with
ensure that
    { when { IUT is requested to send INFORMATIONAL_request
                 containing Delete_payload }
       then { IUT sends INFORMATIONAL request
                  containing IKE_Header
              and containing (Encrypted payload
                             containing Delete_payload
                                         containing Protocol_ID indicating 1
                                     and containing SPI_Size indicating 0
                                     and not containing SPI) }
```

	Test Purpose		
Identifier:	TP_SEC_6014_02		
Summary:	Test of generating INFORMATIONAL_request with Delete payload for CHILD_SA		
References:	RQ_002_6014, RQ_002_6016, RQ_002_6060, RQ_002_6061, RQ_002_6415,RQ_002_6416,		
	RQ_002_6417		
IUT Role:	Host Test Case: TC_SEC_6014_02		
} ensure that { when { IUI	I is requested to send INFORMATIONAL_request containing Delete_payload }		
	I sends INFORMATIONAL_request containing IKE_Header d containing (Encrypted_payload containing Delete_payload containing Protocol_ID indicating 2 or 3 and containing SPI_Size indicating 4 and containing SPI) }		

A.3.4 IKE Protocol

A.3.4.1 Authentication

A.3.4.1.1 Extensible Authentication Methods

		Test Purpose		
Identifier:	TP_SEC_6151_01	P_SEC_6151_01		
Summary:	Test of generating IKE_	Test of generating IKE_AUTH request for extensible authentication methods, message 3		
References:	RQ_002_6151			
IUT Role:	Host	Test Case:	TC_SEC_6151_01	
ensure that { when { IU then { IU th	and IUT having recei	iest	ds'	

	Test Purpose			
Identifier:	P_SEC_6152_01			
Summary:	est reaction on IKE_AUTH request for extensible authentication methods, message 3			
References:	RQ_002_6152, RQ_002_6153			
IUT Role:	Host Test Case: TC_SEC_6152_01			
with { ordered (IUT having received IKE_SA_INIT_request			
	and IUT having sent IKE_SA_INIT_response)			
and IUT co	onfigured 'to support extensible authentication methods'			
}				
ensure that				
$\{$ when $\{$	IUT receives IKE AUTH request			
	not containing Authentication payload }			
then {	IUT sends IKE AUTH response			
	containing Extensible Authentication Protocol payload			
	and containing Identification payload			
	and containing Authentication payload			
and	ot containing Security Association payload			
and	d not containing any Traffic Selector payload }			
}	,			

_	Test Purpose			
Identifier:	TP_SEC_6153_01			
Summary:	Test of generating IKE_AUTH request for extensi	Test of generating IKE_AUTH request for extensible authentication methods, message 5		
References:	RQ_002_6153			
IUT Role:	Host Test Case:	TC_SEC_6153_01		
$\left. ight.\}$ ensure that $\left\{ ight.$ when $\left\{ ight.$ IU	IUT having sent IKE_SA_INIT_request and IUT having received IKE_SA_INIT_respo and IUT having sent IKE_AUTH_request and IUT having received IKE_AUTH_response onfigured 'to use extensible authenticatio T is requested to send IKE_AUTH_request } T sends IKE_AUTH_request containing Extensible_Authentication_Pro	'message 3' 'message 4')		

```
Test Purpose
Identifier:
                   TP SEC 6161 01
Summary:
                   Test reaction on IKE_AUTH request for extensible authentication methods, message 5
References:
                  RQ 002 6161
IUT Role:
                                                                                TC_SEC_6161_01
                  Host
                                                 Test Case:
                  IUT having received IKE_SA_INIT_request and IUT having sent IKE_SA_INIT_response
with { ordered (
                                                                    'message 1
                                                                    'message 2'
                  and IUT having received IKE_AUTH_request
                                                                   'message 3'
                  and IUT having sent IKE_AUTH_response
                                                                   'message 4')
       and IUT having completed 'authentication method successfully'
ensure that
     { when { IUT receives IKE AUTH request
                   containing Extensible Authentication Protocol payload }
       then { IUT sends IKE AUTH response
                   containing (Extensible_Authentication_Protocol_payload
                                containing Code set to 3 'success'
```

```
Test Purpose
                  TP SEC 6162 01
Identifier:
                  Test reaction on IKE_AUTH request for extensible authentication methods, message 5
Summary:
References:
                  RQ 002 6162, RQ 002 6374
IUT Role:
                                               Test Case:
                                                                            TC SEC 6162 01
                 Host
with { ordered (
                     IUT having received IKE_SA_INIT_request
                                                                  'message 1
                 and IUT having sent IKE_SA_INIT_response
                                                                  'message 2'
                 and IUT having received IKE_AUTH_request
                                                                  'message 3'
                 and IUT sent IKE AUTH response
                                                                  'message 4')
       and IUT having completed 'authentication method unsuccessfully'
ensure that
     { when { IUT receives IKE_AUTH_request
                  containing Extensible Authentication Protocol payload }
       then { IUT sends IKE_AUTH_response
                  containing (Notify_payload
                               containing Notify_Message_Type
                                   set to 24 AUTHENTICATION_FAILED) }
```

		Test Purpose		
Identifier:	TP_SEC_6164_01	-		
Summary:	Test of generating IKE_AUTH	I request for extensible au	thentication methods, message 7	
References:	RQ_002_6164			
IUT Role:	Host	Test Case:	TC_SEC_6164_01	
with { ordered (IUT having sent IKE_S	SA_INIT_request	'message 1'	
	and IUT having received	KE_SA_INIT_response	'message 2'	
	and IUT having sent IKE	AUTH request	'message 3'	
	and IUT having received	KE_AUTH response	'message 4'	
	and IUT having sent IKE_A	AUTH_request	'message 5'	
	and IUT having received	KE_AUTH_response	'message 6')	
and IUT 'n	ready to finalize extensib	ole authentication'		
}				
ensure that				
{ when { IU]	T is requested to send IKE	E_AUTH_request }		
then { IU7	then { IUT sends IKE AUTH request			
	containing Authentication	on_payload }		
}				

```
Test Purpose
Identifier:
                  TP SEC 6164 02
Summary:
                  Test reaction on IKE_AUTH request for extensible authentication methods, message 7
References:
                  RQ 002 6164
IUT Role:
                                                                               TC_SEC_6164_02
                  Host
                                                Test Case:
                  IUT having received IKE_SA_INIT_request and IUT having sent IKE_SA_INIT_response
with { ordered (
                                                                     'message 1
                                                                     'message 2'
                  and IUT having received IKE_AUTH_request
                                                                    'message 3'
                  and IUT having sent IKE_AUTH_response
                                                                    'message 4'
                  and IUT having received IKE AUTH request
                                                                     'message 5'
                  and IUT having sent IKE_AUTH_response
                                                                    'message 6' )
       and IUT having completed 'authentication method successfully'
ensure that
     { when { IUT receives IKE AUTH request
                   containing Authentication_payload }
       then { IUT sends IKE_AUTH_response
                   containing Authentication payload
               and containing Security_Association_payload
               and containing Traffic_Selector_payload_initiator
                                      'Next Payload field of previous
                                       payload has value 44'
               and containing Traffic_Selector payload responder
                                      'Next Payload field of previous
                                        payload has value 45' }
```

A.3.4.2 Error Handling

	٦	Test Purpose		
Identifier:	TP_SEC_6186_01			
Summary:	Test reaction on badly formatted I	Fest reaction on badly formatted IKE_SA_INIT request		
References:	RQ_002_6186			
IUT Role:	Host	Test Case:	TC_SEC_6186_01	
and IUT re	receive IKE_SA_INIT_response to send IKE_SA_INIT_response to send IKE_SA_INIT_response containing Notify_payload }	onse		

```
Test Purpose
Identifier:
                 TP SEC 6186 02
Summary:
                 Test reaction on badly formatted IKE_AUTH request
References:
                 RQ_002_6186
IUT Role:
                                                                            TC_SEC_6186_02
                                              Test Case:
                 Host
with { ordered (
                     IUT having received IKE SA INIT request
                 and IUT having sent IKE_SA_INIT_response
ensure that
     { when { IUT receives badly formatted IKE_AUTH_request }
       then { IUT sends IKE AUTH response
                  containing Notify payload }
```

		Test Purpose		
Identifier:	TP_SEC_6188_02	TP_SEC_6188_02		
Summary:	Test reaction on badly	Test reaction on badly formatted IKE_AUTH response		
References:	RQ_002_6188			
IUT Role:	Host	Test Case:	TC_SEC_6188_02	
	and IUT having rec and IUT having sen	<pre>t IKE_SA_INIT_request eived IKE_SA_INIT_response t IKE_AUTH_request) rmatted IKE_AUTH_response } }</pre>		

		Test Purpose		
Identifier:	TP_SEC_6189_01			
Summary:	Test reaction on request outside of known IKE_SA			
References:	•	RQ_002_6189, RQ_002_6190, RQ_002_6191		
IUT Role:	Host	Test Case:	TC_SEC_6189_01	
with { IUT havin	g no IKE_Security_Ass	sociation	 	
}				
ensure that	_		,	
,	-	ILD_SA_request on UDP_port_5	,	
then { IU		_SA_response on UDP_port_500		
	containing destinat	_		
	set to source_a			
		i_in CREATE_CHILD_SA_request		
an	d containing (IKE_Hea			
		ning IKE_SA_Initiators_SPI		
	set	t to IKE_SA_Initiators_SPI		
		received in CREATE_CHIL	D_SA_request	
		ning IKE_SA_Responders_SPI		
	set	t to IKE_SA_Responders_SPI	D 63	
		received in CREATE_CHIL	D_SA_request	
		ning Message_ID		
	set	t to Message_ID	D 63	
		received in CREATE_CHIL	D_SA_request)	
	d not containing an I		1	
an		_payload Not encrypt	cea	
		ning Notify_Message_Type		
ì	set	t to 4 INVALID_IKE_SPI) }		

```
Test Purpose
Identifier:
                 TP SEC 6189 02
                 Test reaction on request outside of known IKE_SA
Summary:
References:
                 RQ_002_6189, RQ_002_6190, RQ_002_6191
IUT Role:
                 Host
                                              Test Case:
                                                                           TC_SEC_6189_02
with { IUT having no IKE_Security_Association
ensure that
    { when { IUT receives INFORMATIONAL_request on UDP_port_4500 }
       then { IUT sends INFORMATIONAL_response on UDP_port_4500
                  containing destination_address
                      set to source address received in INFORMATIONAL request
              and containing (IKE Header
                              containing IKE SA Initiators SPI
                                  set to IKE SA Initiators SPI
                                         received in INFORMATIONAL_request
                          and containing IKE_SA_Responders_SPI
                                  set to IKE SA Responders SPI
                                          received in INFORMATIONAL request
                          and containing Message\_ID
                                  set to Message_ID
                                         received in INFORMATIONAL request
              and not containing an Encrypted_payload
              and containing (Notify_payload
                                                  -- Not encrypted
                              containing Notify Message Type
                                  set to 4 INVALID_IKE_SPI) }
```

	1	Test Purpose	
Identifier:	TP_SEC_6023_01		
Summary:	Test reaction on cryptographically unprotected response indicating invalid SPI		
References:	RQ_002_6023, RQ_002_6194		
IUT Role:	Host	Test Case:	TC_SEC_6023_01
ensure that { when { IUI and	and containing unknows of the containing an Encrypted containing (Notify_payload containing Notify_	sponse wm IKE_SA_Initiators_S wm IKE_SA_Responders_S _payload Not encrypted	

```
Test Purpose
Identifier:
                 TP_SEC_6023_02
                 Test reaction on cryptographically unprotected response indicating invalid SPI
Summary:
References:
                 RQ 002 6023, RQ 002 6194
IUT Role:
                                               Test Case:
                                                                            TC_SEC_6023_02
                 Host
with { IUT having established an IKE Security Association
ensure that
     { when { IUT receives INFORMATIONAL_response
                  containing (IKE Header
                               containing unknown IKE SA Initiators SPI
                          and containing unknown IKE_SA_Responders_SPI)
              and not containing an Encrypted_payload
              and containing (Notify payload
                                                   -- Not encrypted
                              containing Notify_Message_Type
                                  set to 4 INVALID_IKE_SPI) }
       then { IUT sends no response }
```

```
Test Purpose
Identifier:
                  TP_SEC_6023_03
Summary:
                  Test reaction on INFORMATIONAL_request with Notify payload without cryptographic protection
References:
                  RQ_002_6023, RQ_002_6022
IUT Role:
                                               Test Case:
                                                                             TC_SEC_6023_03
                  Host
with { IUT having established an IKE_Security_Association
ensure that
     { when { IUT receives INFORMATIONAL_request
              not containing an Encrypted_payload
                   containing (Notify_payload
                                                    -- Not encrypted
                               containing Notify_Message_Type
                                   set to 4 INVALID IKE SPI) }
       then { IUT sends no INFORMATIONAL_response \overline{\ \ }
```

A.3.4.3 General Protocol Handling

A.3.4.3.1 Address and Port Agility

	Test P	urpose		
Identifier:	TP_SEC_6206_01			
Summary:	Test reaction on IKE_SA_INIT request re	Test reaction on IKE_SA_INIT request received from UDP port other than 500 or 4 500		
References:	RQ_002_6206, RQ_002_6131, RQ_002	_6212		
IUT Role:	Host Test (Case:	TC_SEC_6206_01	
,	eady to receive IKE_SA_INIT_request			
and IUT re	eady to send IKE_SA_INIT_response			
}				
ensure that				
{ when { IUT	Treceives IKE_SA_INIT_request not			
	and not	<pre>from UDP_port_4500 }</pre>		
then { IUT	T sends IKE SA INIT response on 'UDP port from which request			
	Wa	s received' }		
}				

A.3.4.3.2 IP Compression (IPComp)

```
Test Purpose
                  TP_SEC_6385_01
Identifier:
Summary:
                  Test reaction on CREATE_CHILD_SA request with compression offer
References:
                  RQ_002_6385, RQ_002_6203
                                                                               TC_SEC_6385_01
                  Host
                                                 Test Case:
with { IUT having established an IKE_Security_Association
ensure that
     { when { IUT receives CREATE CHILD SA request
                   containing IKE Header
               and containing (Notify_payload
                                containing Notify_Message_Type
    set to 16387 IPCOMP_SUPPORTED
                            and containing (Notification_Data
                                             containing transform_ID)
               and containing additional (Notify_payload
                                containing Notify_Message_Type
                                    set to 16387 IPCOMP SUPPORTED
                            and containing (Notification Data
                                             containing transform_ID) }
       then { IUT sends CREATE CHILD SA response
                   containing IKE Header
               and optionally (containing (Notify_payload
                                             containing Notify_Message_Type
set to 16387 IPCOMP_SUPPORTED
                                         and containing (Notification_Data
                                                     containing 1 transform ID
                                                        received in
                                                        CREATE CHILD SA request)
               and not containing additional (Notify payload
                                                containing Notify_Message_Type
                                                    set to 16387 IPCOMP SUPPORTED) }
```

A.3.4.3.3 Message Format

```
Test Purpose
Identifier:
                 TP SEC 6369 01
Summary:
                 Test reaction on request with incorrect Message ID
                 RQ_002_6369, RQ_002_6370
References:
IUT Role:
                                                                            TC_SEC_6369_01
                 Host
                                              Test Case:
with { IUT having established an IKE Security Association
ensure that
     { when {
                  IUT receives CREATE CHILD SA request
                      containing (IKE Header
                                  containing Message ID 'out of sequence') }
                  IUT not sends CREATE CHILD SA response
       then {
                  and IUT optionally sends INFORMATIONAL request
                      containing (Notify_payload
                                  containing Notify Message Type
                                       set to 9 INVALID_MESSAGE_ID) }
```

```
Test Purpose
Identifier:
                  TP_SEC_6369_02
Summary:
                  Test reaction on request with incorrect Message ID
References:
                  RQ_002_6369, RQ_002_6370
IUT Role:
                                                Test Case:
                                                                               TC_SEC_6369_02
                  Host
with { IUT having established an IKE_Security_Association
ensure that
     \{ \  \, \mathtt{when} \  \, \{
                  IUT receives INFORMATIONAL_request
                      containing (IKE_Header
                                    containing Message_ID 'out of sequence' }
       \verb|then| \{
                  IUT not sends INFORMATIONAL_response
                   and IUT optionally sends INFORMATIONAL request
                             containing (Notify_payload
                                          containing Notify_Message_Type
                                               set to 9 INVALID_MESSAGE_ID) }
```

A.3.4.3.4 Overlapping Requests

	Test Purpose			
Identifier: TP_SEC_6041	_01			
Summary: Test reaction or	est reaction on request when sent request is not answered			
References: RQ_002_6041				
IUT Role: Host	Test Case:	TC_SEC_6041_01		
<pre>and IUT having sent CRE and IUT not having rece } ensure that { when { IUT receives CRE</pre>	hed IKE_Security_Association ATE_CHILD_SA_request ived CREATE_CHILD_SA_response ATE_CHILD_SA_request } _CHILD_SA_response }			

	Test Purpose		
Identifier: TP_SEC_60	41_02		
Summary: Test reaction	Test reaction on request when sent request is not answered		
References: RQ_002_60	41		
IUT Role: Host	Test Case:	TC_SEC_6041_02	
and IUT having sent and IUT not having real and IUT not having real and IUT not having real and IUT receives in the second secon	lished an IKE_Security_Association INFORMATIONAL_request eceived INFORMATIONAL_response INFORMATIONAL_request } DRMATIONAL_response }		

A.3.4.3.5 Request Internal Address

```
Test Purpose
Identifier:
                 TP_SEC_6177_01
Summary:
                 Test reaction on IKE_AUTH request with Configuration Payload
References:
                 RQ_002_6177, RQ_002_6178, RQ_002_6183, RQ_002_6462, RQ_002_6465
IUT Role:
                 Ipsec_gateway
                                             Test Case:
                                                                           TC_SEC_6177_01
with { IUT configured 'to expect IKE_AUTH request to include
                       the Configuration Payload'
ensure that
    { when { IUT receives IKE AUTH request
                  containing (Configuration_payload
                              containing Configuration_Type
                                 set to 1 CFG REQUEST
                          and containing (Configuration_Attribute
                                          containing Attribute_Type
                                              set to 8 INTERNAL_IP6_ADDRESS }
       then { IUT sends IKE_AUTH_response
                  containing (Configuration Payload
                              containing Configuration Type
                                  set to 2 CFG REPLY
                          and containing (Configuration_Attribute
                                          containing Attribute Type
                                             set to 8 INTERNAL IP6 ADDRESS
                                      and containing Attribute_Value
                                              set to IPv6 Address)
                      before the Security_Association_payload }
```

	7	Test Purpose	
Identifier:	TP_SEC_6184_01		
Summary:	Test reaction on IKE_AUTH reque	st without Configuration	on Payload
References:	RQ_002_6184, RQ_002_6462		
IUT Role:	lpsec_gateway	Test Case:	TC_SEC_6184_01
with { IUT config	gured 'to expect IKE_AUTH requ		
	the Configuration Paylo	oad'	
}			
ensure that			
{ when { IUT	receives IKE_AUTH_request		
	not containing (Configuration		
	containing (Configuration_Type	
	set to 1	L CFG REQUEST }	
then { IUT	sends IKE AUTH response		
	containing (Notify payload		
	containing Notin	Ty Message Type	
	set to 37 FA	AILED CP REQUIRED)	}
}			•

A.3.4.3.6 Retransmission Timers

```
Test Purpose
Identifier:
                 TP_SEC_6030_01
Summary:
                 Test reaction on repeated IKE_SA_INIT request
                 RQ_002_6030, RQ_002_6046
References:
                                             Test Case:
IUT Role:
                                                                           TC_SEC_6030_01
                 Host
with { ordered (
                     IUT having received IKE_SA_INIT_request
                 and IUT having sent IKE_SA_INIT_response
ensure that
     { when { IUT receives previous IKE_SA_INIT_request -- i.e. the same as the
                                                         -- one that it has
                                                         -- already answered
       then { IUT resends previous IKE SA INIT response }
```

```
Test Purpose
Identifier:
                    TP_SEC_6030_02
                     Test reaction on repeated IKE_AUTH request
Summary:
References:
                    RQ_002_6030, RQ_002_6046
IUT Role:
                                                      Test Case:
                                                                                         TC_SEC_6030_02
                    Host
                    IUT having received IKE_AUTH_request and IUT having sent IKE_AUTH_response)
with { ordered (
ensure that
     { when { IUT receives previous IKE_AUTH_request -- i.e. the same as the -- one that it has -- already answered
        then { IUT resends previous IKE_AUTH_response }
```

	1	Test Purpose	
Identifier:	TP_SEC_6030_03		
Summary:	Test reaction on repeated CREAT	E_CHILD_SA reques	st
References:	RQ_002_6030, RQ_002_6046		
IUT Role:	Host	Test Case:	TC_SEC_6030_03
}	IUT having received CREAT and IUT having sent CREATE_CH receives previous CREATE_CH resends previous CREATE_CHI	HILD_SA_response) ILD_SA_request	

	Test Purpose		
Identifier:	TP_SEC_6030_04		
Summary:	est reaction on repeated INFORMATIONAL request		
References:	RQ_002_6030, RQ_002_6046		
IUT Role:	Host Test Case: TC_SEC_6030_04		
<pre>with { ordered (</pre>	IUT having received INFORMATIONAL_request and IUT having sent INFORMATIONAL_response) T receives previous INFORMATIONAL_request i.e. the same as the one that it has already answered		
then { IUI	T resends previous INFORMATIONAL_response }		

	Test Purpose			
Identifier:	TP_SEC_6033_01	TP_SEC_6033_01		
Summary:	Test resending of unanswered IKE	SA_INIT request		
References:	RQ_002_6033, RQ_002_6045			
IUT Role:	Host	Test Case:	TC_SEC_6033_01	
with { IUT having sent IKE_SA_INIT_request } ensure that { when { IUT receives no IKE_SA_INIT_response } then { IUT resends previous IKE SA_INIT_request }				
}	resents previous int_bA_inti	reducate)		

	Test Purpose			
Identifier:	TP_SEC_6033_04	TP_SEC_6033_04		
Summary:	Test resending of unanswered IN	Test resending of unanswered INFORMATIONAL request		
References:	RQ_002_6033, RQ_002_6045	RQ 002 6033, RQ 002 6045		
IUT Role:	Host	Test Case:	TC_SEC_6033_04	
<pre>with { IUT having sent INFORMATIONAL_request }</pre>				
<pre>ensure that</pre>				

A.3.4.3.7 Version Compatibility

```
Test Purpose
Identifier:
                  TP_SEC_6065_01
Summary:
                  Test reaction on IKE_SA_INIT request with major version > 2
References:
                  RQ_002_6065, RQ_002_6066, RQ_002_6237
                                                Test Case:
IUT Role:
                  Host
                                                                              TC_SEC_6065_01
with { IUT ready to establish a Security_Association using IKEv2
ensure that
     \{ \  \, \text{when} \  \, \{
                   IUT receives IKE_SA_INIT_request
                       containing (IKE_Header
                                    containing Major_Version
                                       set to greater than 2) }
                   IUT discards IKE_SA_INIT_request
       then {
               and optionally (
                   IUT sends IKE SA INIT response
                       containing (Notify_payload
                                    containing Notify_Message_Type
                                        set to 5 INVALID_MAJOR_VERSION) }
```

```
Test Purpose
                   TP_SEC_6065_02
Identifier:
Summary:
                   Test reaction on IKE_AUTH request with major version > 2
References:
                   RQ_002_6065, RQ_002_6066, RQ_002_6237
IUT Role:
                                                  Test Case:
                                                                                   TC_SEC_6065_02
                   Host
                   IUT having received IKE_SA_INIT_request and IUT having sent IKE_SA_INIT_response)
with { ordered (
ensure that
     \{ \  \, \text{when} \  \, \{
                  IUT receives IKE AUTH request
                        containing (IKE_Header
                                      containing Major_Version
                                         set to greater than 2) }
        then {
                    IUT discards IKE AUTH request
               and optionally (
                    IUT sends IKE_AUTH_response
                        containing (Notify_payload
                                      containing Notify_Message_Type
                                          set to 5 INVALID_MAJOR_VERSION) }
```

Summary: Test rea References: RQ_002 IUT Role: Host with { IUT having estab: } ensure that { when { IUT re	C_6065_03 action on CREATE_CHILD_SA request with major vers 2_6065, RQ_002_6066, RQ_002_6237	ion > 2
References: RQ_000 IUT Role: Host with { IUT having estab: } ensure that { when { IUT re		ion > 2
<pre>IUT Role: Host with { IUT having estab: } ensure that { when { IUT re</pre>	0 6065 PO 002 6066 PO 002 6227	····- =
with { IUT having estab: } ensure that { when { IUT re	2_0005, NQ_002_0000, NQ_002_0257	
ensure that { when { IUT re	Test Case:	TC_SEC_6065_03
{ when { IUT re	lished an IKE_Security_Association	
and option	cceives CREATE_CHILD_SA_request containing (IKE_Header	}

	7	est Purpose	
Identifier:	TP_SEC_6065_04		
Summary:	Test reaction on INFORMATIONA	L_request with major version	> 2
References:	RQ_002_6065, RQ_002_6066, R0	Q_002_6237	
IUT Role:	Host	Test Case:	TC_SEC_6065_04
with { IUT having	established an IKE_Security	Association	
}			
ensure that			
{ when {	IUT receives INFORMATIONAL_1	request	
	containing (IKE_Header		
	containing Major_Version		
	set to greater than 2 }		
then {	IUT discards INFORMATIONAL_request		
and	optionally (
	IUT sends INFORMATIONAL response		
	containing (Notify payload		
	containing 1	Notify Message Type	
	set to 5 INVALID MAJOR VERSION) }		
}			,

```
Test Purpose
Identifier:
                 TP SEC 6068 01
Summary:
                 Test reaction on IKE_SA_INIT request with major version < 2
References:
                 RQ_002_6068, RQ_002_6067, RQ_002_6069
IUT Role:
                                                                            TC_SEC_6068_01
                 Host
                                              Test Case:
with { IUT ready to establish a Security_Association using IKEv2
ensure that
     { when { IUT receives IKE_SA_INIT_request
                  containing (IKE_Header
                               containing Major_Version set to 1) }
       then { IUT sends IKE_SA_INIT_response
                  containing (IKE Header
                               containing Major Version set to 1
                          and containing V_Bit set to 1) }
```

	Test Purpose		
Identifier:	TP_SEC_6068_02		
Summary:	Test reaction on IKE_AUTH request with major version < 2		
References:	RQ_002_6068, RQ_002_6067, RQ_002_6069		
IUT Role:	Host Test Case:	TC_SEC_6068_02	
with { ordered (<pre>IUT having sent IKE_SA_INIT_request</pre>		
	<pre>and IUT having received IKE_SA_INIT_response)</pre>		
}			
ensure that			
{ when { IUT	receives IKE AUTH request		
	containing (IKE_Header		
	containing Major Version set to 1) }		
then { IUT	then { IUT sends IKE AUTH response		
	containing (IKE_Header		
	containing Major_Version set to 1		
	and containing V Bit set to 1) }		
}			

	1	Test Purpose	
Identifier:	TP_SEC_6068_03		
Summary:	Test reaction on CREATE CHILD SA request with major version < 2		
References:	RQ_002_6068, RQ_002_6067, R0	Q_002_6069	
IUT Role:	Host	Test Case:	TC_SEC_6068_03
ensure that { when { IUT	Sends CREATE_CHILD_SA_respond containing (IKE_Header	quest r_Version set to 1) nse r_Version set to 1	}

```
Test Purpose
Identifier:
                 TP_SEC_6068_04
Summary:
                 Test reaction on INFORMATIONAL_request with major version < 2
                 RQ_002_6068, RQ_002_6067, RQ_002_6069
References:
IUT Role:
                                              Test Case:
                                                                           TC_SEC_6068_04
                 Host
with { IUT having established an IKE_Security_Association
ensure that
     { when { IUT receives INFORMATIONAL_request
                  containing (IKE_Header
                              containing Major_Version set to 1) }
       then { IUT sends INFORMATIONAL response
                  containing (IKE_Header
                              containing Major_Version set to 1
                          and containing V Bit set to 1) }
```

```
Test Purpose
                 TP_SEC_6362_01
Identifier:
                 Test reaction on CREATE_CHILD_SA request with unrecognized payload
Summary:
References:
                 RQ_002_6362, RQ_002_6255
IUT Role:
                                              Test Case:
                                                                          TC_SEC_6362_01
                 Host
with { IUT having established an IKE_Security_Association
ensure that
     { when { IUT receives CREATE_CHILD_SA_request
                 containing unrecognized (payload
                             containing C_Bit set to 1) }
       then { IUT sends CREATE_CHILD_SA_response
                  containing (Notify payload
                              containing Notify_Message_Type
                                  set to 1 UNSUPPORTED_CRITICAL_PAYLOAD) }
```

	7	Test Purpose	
Identifier:	TP_SEC_6362_02		
Summary:	Test reaction on INFORMATIONAL request with unrecognized payload		
References:	RQ_002_6362, RQ_002_6255		
IUT Role:	Host	Test Case:	TC_SEC_6362_02
ensure that { when { IU	receives INFORMATIONAL_requered containing unrecognized (pay containing C_Bit sends INFORMATIONAL_response containing (Notify_payload containing Notify_payload set to 1 UNS	est yload set to 1) }	AD) }

	7	Test Purpose		
Identifier:	TP_SEC_6073_01			
Summary:	Test reaction on CREATE_CHILD	Test reaction on CREATE_CHILD_SA request with unrecognized payload		
References:	RQ_002_6073, RQ_002_6256			
IUT Role:	Host	Test Case:	TC_SEC_6073_01	
ensure that { when { IU	G established an IKE_Security T receives CREATE_CHILD_SA_recontaining unrecognized (pay containing C_Bit T sends CREATE_CHILD_SA_respond to containing (Notify_payload containing Notify_set to 1 UNS	quest yload set to 0) } nse	AD) }	

	Test Purpose		
Identifier:	TP_SEC_6073_02		
Summary:	Test reaction on INFORMATIONAL_request with unrecognized page	yload	
References:	RQ_002_6073, RQ_002_6256		
IUT Role:	Host Test Case:	TC_SEC_6073_02	
ensure that { when { IUI then { IUI	g established an IKE_Security_Association I receives INFORMATIONAL_request containing unrecognized (payload	}	

A.3.4.4 Security Parameter Negotiation

A.3.4.4.1 Algorithm Negotiation

```
Test Purpose
Identifier:
                 TP_SEC_6088_01
                 Test reaction on IKE_SA_INIT request with several SA proposal
Summary:
                 RQ_002_6088, RQ_002_6271
References:
                                              Test Case:
                                                                           TC_SEC_6088_01
IUT Role:
                 Host
with { IUT ready to establish a Security_Association using IKEv2
ensure that
    { when { IUT receives IKE_SA_INIT_request
                  containing (Security_Association_payload
                              containing at least 1 acceptable Proposal ) }
       then { IUT sends IKE SA INIT response
                  containing (Security_Association_payload
                              containing 1 Proposal)
```

	7	Test Purpose		
Identifier:	TP_SEC_6088_02			
Summary:	Test reaction on IKE_AUTH reque	Test reaction on IKE_AUTH request with several SA proposal		
References:	RQ_002_6088, RQ_002_6271			
IUT Role:	Host	Test Case:	TC_SEC_6088_02	
and IUT h	aving sent IKE_SA_INIT_request aving received IKE_SA_INIT_res T receives IKE_AUTH_request containing (Security_Association to the containing at 10) T sends IKE_AUTH_response containing 1 Process containing 1 P	sponse ation_payload east 1 acceptable ation_payload	Proposal) }	

	Tes	t Purpose	
Identifier:	TP_SEC_6088_03		
Summary:	Test reaction on CREATE_CHILD_SA	A request with several SA pro	pposal
References:	RQ_002_6088, RQ_002_6271		
IUT Role:	Host Tes	st Case:	TC_SEC_6088_03
ensure that { when { IUI	receives CREATE_CHILD_SA_reque containing (Security_Association containing at least sends CREATE_CHILD_SA_response containing (Security_Association (Security_Association containing 1 Propo	st on_payload t 1 acceptable Proposal) on_payload	}
}			

```
Test Purpose
Identifier:
                 TP_SEC_6372_01
Summary:
                 Test reaction on IKE_SA_INIT request with unacceptable SA proposal
References:
                 RQ_002_6372
IUT Role:
                                                                            TC_SEC_6372_01
                 Host
                                               Test Case:
with { IUT ready to establish a Security_Association using IKEv2
ensure that
     { when { IUT receives IKE_SA_INIT_request
                  containing (Security_Association_payload
                               containing no acceptable Proposal) }
       then { IUT sends IKE_SA_INIT_response
                  containing (Notify payload
                              containing Notify_Message_Type
                                  set to 14 NO_PROPOSAL_CHOSEN) }
```

	-	Test Purpose		
Identifier:	TP_SEC_6372_02	TP_SEC_6372_02		
Summary:	Test reaction on IKE_AUTH reque	Test reaction on IKE_AUTH request with unacceptable SA proposal		
References:	RQ_002_6372			
IUT Role:	Host	Test Case:	TC_SEC_6372_02	
	aving sent IKE_SA_INIT_reques			
and IUT ha	aving received IKE_SA_INIT_re	sponse		
ensure that				
{ when { IU	n { IUT receives IKE_AUTH_request			
	containing (Security_Association_payload			
<pre>containing no acceptable Proposal) }</pre>				
then { IUT sends IKE_AUTH_response				
	<pre>containing (Notify_payload</pre>			
containing Notify_Message_Type				
	set to 14 N	O_PROPOSAL_CHOSEN)	}	
}				

Test Purpose					
Identifier:	TP_SEC_6372_03				
Summary:	Test reaction on CREATE_CHILD_SA request with unacceptable SA proposal				
References:	RQ 002 6372				
IUT Role:	Host	Test Case:	TC_SEC_6372_03		
<pre>with { IUT having established an IKE_Security_Association } ensure that { when { IUT receives CREATE_CHILD_SA_request</pre>					

```
Test Purpose
Identifier:
                  TP_SEC_6373_01
                   Test reaction on IKE_SA_INIT request with invalid Diffie-Hellman value
Summary:
References:
                  RQ_002_6373, RQ_002_6306
IUT Role:
                                                                                 TC_SEC_6373_01
                  Host
                                                 Test Case:
with { IUT ready to establish a Security_Association using IKEv2
ensure that
     { when { IUT receives IKE_SA_INIT_request
                   containing (Key_Exchange_payload
                                containing an invalid DH Group number) }
       then { IUT sends IKE_SA_INIT_response containing (Notify_payload
                                containing Notify_Message_Type
                                     set to 17 INVALID_KE_PAYLOAD) }
```

A.3.4.4.2 Cookies

```
Test Purpose
Identifier:
                 TP_SEC_6081_01
Summary:
                 Test reaction on IKE_SA_INIT response with COOKIE Notify payload
References:
                 RQ 002 6081, RQ 002 6080, RQ 002 6391
                                                                           TC_SEC_6081_01
IUT Role:
                 Host
                                              Test Case:
with { IUT having sent IKE_SA_INIT_request
ensure that
     { when { IUT receives IKE_SA_INIT_response
                  containing (Notify_payload
                              containing Notify_Message_Type
                                  set to 16390 COOKIE
                          and containing (Notification_Data
                                          containing 'Cookie data') }
       then { IUT sends IKE_SA_INIT_request
                  containing (Notify_payload
                              containing Notify_Message_Type
                                  set to 16390 COOKIE
                          and containing Notification Data
                                  set to Notification_Data
                                         received in IKE_SA_INIT_response)
              and containing 'all other payloads from initial
                              request unchanged' }
```

A.3.4.4.3 Rekeying

Test Purpose					
Identifier:	TP_SEC_6101_01				
Summary:	Test of generating CREATE_CHILD_SA request for rekeying of child SA				
References:	RQ_002_6101, RQ_002_6172, RQ_002_6173, RQ_002_6397				
IUT Role:	Host Test Case:	TC_SEC_6101_01			
with { IUT ha	ving established an IKE_Security_Association				
and IUT ha	ving established a CHILD SA				
and IUT 'h	aving detected that the lifetime of the CHILD_SA				
i	is about to expire'				
and IUT 'able to rekey CHILD SA within IKE SA'					
}					
ensure that					
{ when { IUT is requested to send CREATE CHILD SA request }					
then { IUT sends CREATE CHILD SA request					
containing (Notify payload					
	containing Notify Message Type				
	set to 16393 REKEY SA) }				
}	_ ,				

```
Test Purpose
Identifier:
                  TP SEC 6102 01
Summary:
                  Test of deletion of old CREATE_CHILD_SA after rekeying
References:
                  RQ_002_6102
IUT Role:
                                                 Test Case:
                                                                                TC_SEC_6102_01
                  Host
            IUT having established an IKE_Security_Association
with {
       and IUT having established a CHILD SA
       and IUT 'having detected that the lifetime of the CHILD SA
                 was about to expire'
       and IUT having sent CREATE_CHILD_SA_request 'for rekeying'
ensure that
       when { IUT receives CREATE_CHILD_SA_response }
       then { IUT sends INFORMATIONAL_request
                   containing (Delete_payload
                                containing Security_Parameters_Index
indicating CHILD_SA 'to be deleted') }
```

```
Test Purpose
Identifier:
                 TP SEC 6103 01
Summary:
                 Test of generating CREATE_CHILD_SA request for rekeying of IKE SA
References:
                 RQ_002_6103
IUT Role:
                                              Test Case:
                                                                           TC_SEC_6103_01
                 Host
           IUT having established an IKE_Security_Association
with {
       and IUT having established a CHILD_SA
       and IUT 'having detected that the lifetime of the IKE_SA
                was about to expire'
     }
ensure that
     { when { IUT is requested to send CREATE_CHILD_SA_request }
       then { IUT sends CREATE CHILD SA request
              not containing Traffic Selector payload initiator
              and not containing Traffic_Selector_payload_responder }
```

```
Test Purpose
Identifier:
                 TP_SEC_6105_01
                 Test of deletion of old IKE_SA after rekeying
Summary:
References:
                 RQ_002_6105
IUT Role:
                                                                            TC_SEC_6105_01
                 Host
                                              Test Case:
with {
           IUT having established an IKE_Security_Association
       and IUT having established a CHILD SA
       and IUT 'having detected that the lifetime of the CHILD_SA
                was about to expire'
       and IUT 'has rekeyed IKE_SA'
ensure that
     { when { IUT is requested to send INFORMATIONAL_request }
       then { IUT sends INFORMATIONAL_request
                  containing (Delete_payload
                              containing Security_Parameters_Index
                              indicating IKE_Security_Association
                                         'to be deleted') }
```

A.3.4.4.4 Traffic Selector Negotiation

Test Purpose					
ldentifier:	TP_SEC_6123_01				
Summary:	Test reaction on CREATE_CHILD_SA request with acceptable and unacceptable traffic selectors				
References:	RQ_002_6123				
IUT Role:	Host Test Case:	TC_SEC_6123_01			
with { IUT having	sestablished an IKE_Security_Association				
}					
ensure that					
$\{$ when $\{$ IU $\}$	receives CREATE_CHILD_SA_request				
	<pre>containing (Traffic_Selector_payload_initiat</pre>	tor			
	containing first				
	<pre>and acceptable Traffic_Se</pre>	elector			
	and containing next				
	and unacceptable Traffic_S	Selector)			
and	l containing (Traffic_Selector_payload_respond	der			
	containing first				
	and acceptable Traffic_Se	elector			
	and containing next				
	and unacceptable Traffic_S	Selector) }			
then { IU	Sends CREATE_CHILD_SA_response				
	<pre>containing (Traffic_Selector_payload_initiat</pre>	tor			
	containing acceptable Traffic_Se	elector			
	received in CREATE_CHILD_SA_re	equest)			
and	l containing (Traffic_Selector_payload_respond				
	containing acceptable Traffic_Se				
	received in CREATE_CHILD_SA_re	equest) }			
}					

```
Test Purpose
Identifier:
                 TP SEC 6125 01
Summary:
                  Test reaction on CREATE_CHILD_SA request with acceptable and unacceptable traffic selectors
References:
                 RQ_002_6125, RQ_002_6383
IUT Role:
                                                                             TC_SEC_6125_01
                 Host
                                               Test Case:
with { IUT having established an IKE_Security_Association
ensure that
     { when { IUT receives CREATE_CHILD_SA_request
                  containing (Traffic_Selector_payload_initiator
                               containing Traffic_Selector
                               indicating 'a range of parameters of which
                                           only a subset is acceptable')
              and containing (Traffic_Selector_payload_responder
                               containing Traffic_Selector
                                   set to 'a range of parameters of which
                                           only a subset is acceptable') }
       then { IUT sends CREATE CHILD SA response
                  containing (Traffic_Selector_payload_initiator
containing Traffic_Selector
                                   set to 'acceptable subset of range'
                                          received in CREATE CHILD SA request)
              and containing (Traffic_Selector_payload_responder
                               containing Traffic_Selector
                                   set to 'acceptable subset of range'
                                          received in CREATE_CHILD_SA_request)
              and optionally (
                  containing (Notify_payload
                               containing Notify_Message_Type
                                   set to 16386 ADDITIONAL_TS_POSSIBLE) }
```

Annex B (informative): Bibliography

- IETF RFC 4301: "Security Architecture for the Internet Protocol".
- IETF RFC 4302: "IP Authentication Header".
- IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".
- IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol".

History

Document history					
V1.1.1	April 2007	Publication			
V1.2.0	April 2008	Publication			