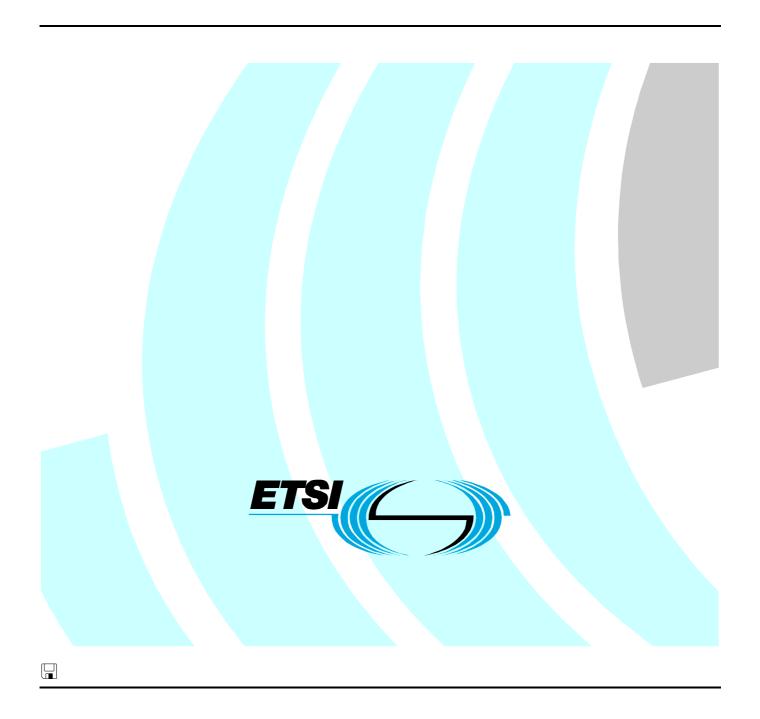
ETSITS 102 593 V1.1.1 (2007-04)

Technical Specification

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



Reference

DTS/MTS-IPT-010-IPv6-SecTSS_TP

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

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 2007.
All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members. **TIPHON**TM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members. **3GPP**TM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intelle	ectual Property Rights	4
Forew	word	4
1	Scope	5
2	References	5
3	Definitions and abbreviations	
3.1 3.2	Definitions	
4	Test Suite Structure (TSS)	6
Anne	ex A (normative): Test Purposes (TP)	8
A.1	Authentication Header (AH)	8
A.2	Encapsulating Security Payload (ESP)	12
A.3	Key Exchange (IKEv2) Protocol	
A.3.1	Exchange Message Structures	
A.3.2	III II	
A.3.2.		
A.3.2.2	J I	
A.3.3 A.3.4	<i>6</i>	
A.3.4.		
A.3.4.		
A.3.4.2		
A.3.4.3	· · · · · · · · · · · · · · · · · · ·	
A.3.4.3		
A.3.4.3	3.6 Retransmission Timers	39
A.3.4.3	3.7 Version Compatibility	41
A.3.4.4	\mathcal{G}	
A.3.4.4	6	
A.3.4.4		
A.3.4.4	· · · · · · · · · · · · · · · · · · ·	
A.3.4.4	4.4 Traffic Selector Negotiation	49
Anne	ex B (informative): Bibliography	51
Histor	ry	52

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

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- 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.
- For a non-specific reference, the latest version applies.

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

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

- [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".

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

RC

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

AH Authentication Header
ATS Abstract Test Suite
ESP Encapsulating Security Payload
IETF Internet Engineering Task Force
IKE Internet Key Exchange
IPv6 Internet Protocol version 6
IUT Implementation Under Test

RQ Requirement
TP Test Purpose
TSS Test Suite Structure
UDP User Datagram Protocol

4 Test Suite Structure (TSS)

Requirements Catalogue

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_102593v010101p0.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_201	17,		
	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			
$oxed{ ext{with}}$ { $oxed{ ext{IUT}}$ ar	nd destination_node established in an AH_security_association			
}				
ensure that				
{ when {	{ IUT is requested to send first unicast IPv6Packet			
	<pre>containing Authentication_Header }</pre>			
then {	{ IUT sends IPv6Packet			
	<pre>containing next_header_field of previous_header</pre>			
	set to 51			
	and containing (Authentication_Header			
	<pre>containing Security_Parameters_Index</pre>			
	set to Security Parameters Index			
	received from destination_node			
	during SA establishment			
	and containing sequence_number set to 1			
	and containing correctly calculated			
	Integrity Check Value			
	<pre>including necessary padding_bits) }</pre>			
}				

```
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
                                                               TC_SEC_2000_02
IUT Role
                                      Test Case:
              Ipsec_host
with { IUT and destination_node established in an AH_security_association
ensure that
     { when { IUT is requested to send subsequent unicast IPv6Packet
                   containing Authentication_Header }
       then { IUT sends IPv6Packet
                   containing next_header_field of previous_header
                        set to 51
               and containing (Authentication_Header
                                containing Security_Parameters_Index
                                     set to Security_Parameters_Index
                                            received from destination_node
                                            during SA_establishment
                            and containing sequence_number set to
                               (sequence_number of previous IPv6Packet) plus 1
                            and containing correctly calculated
                                           Integrity_Check_Value
                                           including necessary padding_bits) }
```

	T	est Purpose			
Identifier:	TP_SEC_2000_03				
Summary:	Test of generating first multicast IF	Pv6 packets with Authentication H	eader		
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, R0	Q_002_2033, RQ_002_2034, RQ	_002_2036		
IUT Role	10000_11000	Test Case:	TC_SEC_2000_03		
with $\{$ IUT es	stablished in a multicast	t_group AH_Security_As:	sociation		
}					
ensure that					
$\{$ when $\{$	IUT is requested to ser	nd first multicast IPv	6Packet		
	containing Authenti	ication_Header }			
then {	IUT sends IPv6Packet				
	containing next_hea	ader_field of previous_	_header		
	set to 51				
	and containing (Authent	tication_Header			
	contair	ning Security_Parameter	rs_Index		
		assigned to multic	cast_group		
		Secur	ity_Association		
	and containing sequence number set to 1				
	and containing correctly calculated				
Integrity_Check_Value			Value		
		including necessa	ary 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
                                      Test Case:
                                                               TC_SEC_2000_04
              Ipsec_host
with { IUT established in multicast_group AH_Security_Association
ensure that
     { when { IUT is requested to send subsequent multicast IPv6Packet
                   containing Authentication_Header }
       then { IUT sends IPv6Packet
                   containing next_header_field of previous_header
                        set to 51
               and containing (Authentication_Header
                                containing Security_Parameters_Index
                                     set to Security_Parameters_Index
                                            assigned to multicast_group
                                                         Security_Association
                            and containing sequence_number set to
                               (sequence_number of previous IPv6Packet) plus 1
                            and containing correctly calculated
                                           Integrity_Check_Value
                                           including necessary padding_bits) }
```

	Test Purpose				
Identifier:	TP_SEC_2009_01				
Summary:	Test reaction on multicast IPv6 p	ackets for unknown multicast_grou	ıp SA		
References:	RQ_002_2009, RQ_002_2008				
IUT Role	lpsec_host	Test Case:	TC_SEC_2009_01		
with { IUT es	stablished in multicast_	group AH_Security_Asso	ciation		
}					
ensure that					
{ when {	IUT receives multicast	: IPv6Packet			
	containing (Auther	ntication_Header			
	contai	ining Security_Paramete	rs Index		
	unrelated to established				
	<pre>multicast_group Security_Association) }</pre>				
then {	IUT discards IPv6Packe	_	, j		
}					

	Test Purpose				
Identifier:	TP_SEC_2042_01	•			
Summary:	Test reaction on IPv6 packets wit	h AH header and fragmentation he	eader		
References:	RQ_002_2042				
IUT Role	lpsec_host	Test Case:	TC_SEC_2042_01		
<pre>IUT Role</pre>					

```
Test Purpose
Identifier:
               TP_SEC_2046_01
               Test reaction on IPv6 packets with AH header when no SA exists
Summary:
References:
              RQ_002_2046
IUT Role
                                       Test Case:
                                                                 TC_SEC_2046_01
              Ipsec_host
with { IUT and destination_node not established in an AH_Security_Association
ensure that
     { when { IUT receives IPv6Packet
                   containing Authentication_Header }
       then { IUT discards IPv6Packet }
```

		Test Purpose		
Identifier:	TP_SEC_2053_01	•		
Summary:	Test reaction on IPv6 packets with	th AH header with incorrect sequer	nce number	
References:	RQ_002_2053			
IUT Role	lpsec_host	Test Case:	TC_SEC_2053_01	
with { IU	JT and destination_node	established in an AH_se	ecurity_association	
and IU	JT and destination_node	'having already exchang	ged	
		at least one packet'		
}				
ensure that				
{ when {	IUT receives IPv6Packe	et		
,	containing (Auther	ntication_Header		
	contai	ining sequence_number		
	set to sequence_number received			
		in previous IPv6packe	_	
then {	IUT discards IPv6Packe	_ <u>-</u>	. ,	

Test Purpose				
Identifier:	TP_SEC_2057_01			
Summary:	Test reaction on IPv6 packets wit	th AH header with correct ICV valu	e	
References:	RQ_002_2057, RQ_002_2028			
IUT Role	lpsec_host	Test Case:	TC_SEC_2057_01	
with { IUT an	nd destination_node esta	ablished in an AH_secur	ity_association	
}				
ensure that				
$\{$ when $\{$	IUT receives IPv6Packe	et		
	containing (Authentication_Header			
	contai	ining Integrity_Check_Va	alue	
	calculated from Security_Association_data			
	<pre>and packet_contents) }</pre>			
then {	then { IUT accepts IPv6Packet }			
}		<u>-</u>		

```
Test Purpose
Identifier:
               TP SEC 2058 01
               Test reaction on IPv6 packets with AH header with incorrect ICV value
Summary:
References:
               RQ_002_2058, RQ_002_2028
IUT Role
              Ipsec_host
                                         Test Case:
                                                                  TC_SEC_2058_01
with { IUT and destination_node established in an AH_security_association
ensure that
     { when { IUT receives IPv6Packet
                    containing (Authentication_Header
                                 containing Integrity_Check_Value
                                 not calculated from Security_Association_data
                                                   and packet_contents) }
        then { IUT discards IPv6Packet }
```

A.2 Encapsulating Security Payload (ESP)

	Test Purpose				
Identifier:	TP_SEC_3030_01				
Summary:	Test reaction on ESP dummy page	cket			
References:	RQ_002_3030				
IUT Role	lpsec_host	Test Case:	TC_SEC_3030_01		
<pre>with { IUT and destination_node established in an ESP_Security_Association } ensure that { when { IUT receives IPv6Packet</pre>					

```
Test Purpose
               TP_SEC_3059_01
Identifier:
               Test reaction on IPv6 packets with ESP header when no SA exists
Summary:
References:
               RQ_002_3059
IUT Role
                                        Test Case:
              Ipsec_host
                                                                  TC_SEC_3059_01
with {
       IUT and destination_node established in an ESP_Security_Association
ensure that
     { when { IUT receives IPv6Packet
                    containing ESP_Header
               and containing (Fragment_Header
                                 containing offset not set to 0) }
       then { IUT discards IPv6Packet }
```

```
Test Purpose
               TP_SEC_3061_01
Identifier:
Summary:
               Test reaction on IPv6 packets with ESP header when no SA exists
References:
               RQ_002_3061, RQ_002_3091
IUT Role
              Ipsec_host
                                         Test Case:
                                                                   TC_SEC_3061_01
with { IUT 'has not established ESP Security Association with destination Node'
ensure that
      { when { IUT receives IPv6Packet
                    containing ESP_Header }
        then { IUT discards IPv6Packet }
```

```
Test Purpose
Identifier:
               TP_SEC_3068_01
               Test reaction on IPv6 packets with ESP header with correct ICV value
Summary:
References:
               RQ_002_3068, RQ_002_3072
                                        Test Case:
                                                                 TC_SEC_3068_01
IUT Role
              lpsec_host
            IUT and destination_node established in an ESP_Security_Association
with {
       and IUT 'having enabled anti-replay service'
ensure that
     { when { IUT receives IPv6Packet
                    containing (ESP_Header
                                 containing sequence_number
                                 set to sequence_number from received IPv6Packet) }
       then { IUT discards IPv6Packet }
```

		Test Purpose		
Identifier:	TP_SEC_3077_01			
Summary:	Test reaction on IPv6 pack	cets with ESP header with corr	ect ICV value	
References:	RQ_002_3077			
IUT Role	lpsec_host	Test Case:	TC_SEC_3077_01	
with {	IUT and destination_	node established in	an ESP_Security_Association	
and 1	ESP_Security_Associa	tion configured to u	se	
	combined_confide	ntiality_and_integri	ty_algorithms	
}				
ensure that				
{ when	{ IUT receives IPv6	Packet		
	containing (E	SP_Header		
	C	ontaining Integrity_	Check_Value	
	calculated from Security_Association_data			
	and packet contents) }			
then	{ IUT accepts IPv6Pa	acket }	_ ,	

		Test Purpose		
Identifier:	TP_SEC_3078_01			
Summary:	Test reaction on IPv6 packets wit	th ESP header with i	ncorrect ICV value	
References:	RQ_002_3078, RQ_002_3077			
IUT Role	lpsec_host	Test Case:	TC_SEC_3078_01	
with { IU	T and destination_node	established i	n an ESP_Security_Association	
and ES	P_Security_Association	configured to	use	
	combined_confidential	lity_and_integ	rity_algorithms	
}				
ensure that				
{ when {	IUT receives IPv6Packe	et		
	containing (ESP He	eader		
	contai	ining Integrit	y Check Value	
	not calculated from Security_Association_data			
	<pre>and packet contents) }</pre>			
then {	IUT discards IPv6Packe		,	

```
Test Purpose
Identifier:
               TP_SEC_3080_01
               Test reaction on IPv6 packets with ESP header with correct ICV value
Summary:
References:
              RQ_002_3080
IUT Role
                                       Test Case:
                                                                TC_SEC_3080_01
              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 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_3083_01	•		
Summary:	Test reaction on IPv6 packets wi	th ESP header with incorrect ICV	value	
References:	RQ_002_3083, RQ_002_3080			
IUT Role	lpsec_host	Test Case:	TC_SEC_3083_01	
with {	UT and destination_node	established in an ESP_	Security_Association	
and E	SP_Security_Association	configured to use		
	separate_confidentia	lity_and_integrity_algo	rithms	
}				
ensure that				
{ when	{ IUT receives IPv6Pack	et		
	containing (ESP_H	eader		
	conta	ining Integrity_Check_V	'alue	
	not calculated from Security_Association_data			
	<pre>and packet_contents) }</pre>			
then }	{ IUT discards IPv6Pack	et }	·	

```
Test Purpose
Identifier:
              TP SEC 3102 01
Summary:
              Test of generating first unicast IPv6 packets with ESP Header, transport mode
References:
              RQ 002 3102, RQ 002 3004, RQ 002 3005, RQ 002 3009, RQ 002 3012, RQ 002 3027,
              RQ_002_3037, RQ_002_3113
                                       Test Case:
IUT Role
                                                               TC_SEC_3102_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 is requested to send first 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 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_3102_02			
Summary:		Test of generating subsequent unicast IPv6 packets with ESP Header, transport mode			
Referenc	es:		, RQ_002_3005, RQ_002_3006,	RQ_002_3009, RQ_002_3027,	
		RQ_002_3037, RQ_002_3112			
IUT Role		lpsec_host	Test Case:	TC_SEC_3102_02	
with {			established in an ESP_	_Security_Association	
	and E	SP_Security_Association			
		separate_confidentia	lity_and_integrity_algo	orithms	
}					
ensure	that				
{	when		end subsequent IPv6Pack	tet in transport_mode	
		containing ESP_He	ader }		
	then	IUT sends IPv6Packet	<pre>in transport_mode</pre>		
		<pre>containing next_h</pre>	eader_field of previous	s_header	
		set to 50			
		and containing (ESP_H	eader		
		conta	<pre>ining Security_Paramete</pre>	ers_Index	
		s	et to Security_Paramete		
			received from des	stination_node	
			during SA_establi	shment	
		and conta	ining sequence_number s	set to	
		(sequ	ence_number of previous	s IPv6Packet) plus 1	
		and conta	ining necessary padding	_bytes	
		and conta	<pre>ining pad_length</pre>		
		s	et to number of padding	_bytes	
	and containing correctly calculated				
			Integrity_Check_Va	ılue	
		inclu	ding necessary padding_	_bits) }	
}					

```
Test Purpose
Identifier:
              TP SEC 3103 01
Summary:
              Test of generating first unicast IPv6 packets with ESP Header, tunnel mode
References:
              RQ 002 3103, RQ 002 3004, RQ 002 3005, RQ 002 3009, RQ 002 3012, RQ 002 3027,
              RQ_002_3037, RQ_002_3092, RQ_002_3113
                                      Test Case:
IUT Role
                                                              TC_SEC_3103_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 is requested to send first 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 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_02	•		
Summary:		Test of generating subsequent unicast IPv6 packets with ESP Header, tunnel mode			
Referenc	es:	RQ_002_3103, RQ_002_3004,	RQ_002_3005, RQ_002_3006,	RQ_002_3009, RQ_002_3027,	
		RQ_002_3037, RQ_002_3092, I	RQ_002_3112		
IUT Role		lpsec_host	Test Case:	TC_SEC_3103_02	
with {		JT and destination_node		Security_Association	
	and E	SP_Security_Association			
		separate_confidentia	lity_and_integrity_algo	orithms	
}					
ensure	that				
{	when	$\left[egin{array}{c} ext{IUT} & ext{is requested to s} ight. \end{array} ight.$		et in tunnel_mode	
		containing ESP_He	ader }		
	then	IUT sends IPv6Packet			
		_	eader_field of previous	_header	
		set to 50	set to 50		
		and containing (ESP_Header			
		conta	ining Security_Paramete	ers_Index	
		s	et to Security_Paramete		
			received from des	tination_node	
			during SA_establi	shment	
			ining sequence_number s		
		(sequ	ence_number <mark>of previous</mark>	IPv6Packet) plus 1	
	and containing necessary padding_bytes			_bytes	
	<pre>and containing pad_length</pre>				
	<pre>set to number of padding_bytes</pre>				
		and conta	ining correctly calcula	ted	
			Integrity_Check_Va	lue	
		inclu	ding necessary padding_	bits) }	
}					

```
Test Purpose
Identifier:
              TP SEC 3107 01
Summary:
              Test of generating first unicast IPv6 packets with ESP Header, transport mode
References:
              RQ 002 3102, RQ 002 3004, RQ 002 3005, RQ 002 3009, RQ 002 3012, RQ 002 3027,
              RQ_002_3113
                                      Test Case:
IUT Role
                                                              TC_SEC_3107_01
             Ipsec_host
with {
            IUT and destination_node established in an ESP_Security_Association
       and ESP_Security_Association configured to use
                combined_confidentiality_and_integrity_algorithms
     }
ensure that
     { when { IUT is requested to send first 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 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_02	-			
Summary:	Test of generating subsequent ur	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				
IUT Role	Ipsec_host	Test Case:	TC_SEC_3107_02		
	JT and destination_node		Security_Association		
and ES	SP_Security_Association	_			
	combined_confidential	lity_and_integrity_algo	rithms		
}					
ensure that					
{ when	$\{$ IUT is requested to se	end subsequent IPv6Pack	et in transport_mode		
	containing ESP_Hea	,			
then -	{ IUT sends IPv6Packet i	- —			
	- -	eader_field of previous	_header		
	set to 50				
	and containing (ESP_He				
	contai	ining Security_Paramete	rs_Index		
	se	et to Security_Paramete			
		received from des	tination_node		
		during SA_establi	shment		
		ining sequence_number s			
	(seque	ence_number of previous	IPv6Packet) plus 1		
		i ning necessary padding	_bytes		
<pre>and containing pad_length</pre>					
	<pre>set to number of padding_bytes</pre>				
	and contai	ining correctly calcula	ted		
		Integrity_Check_Va	lue		
	includ	ling necessary padding_	bits) }		
}					

```
Test Purpose
Identifier:
              TP SEC 3108 01
Summary:
              Test 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
                                       Test Case:
IUT Role
                                                              TC_SEC_3108_01
              Ipsec_host
with {
            IUT and destination_node established in an ESP_Security_Association
       and ESP_Security_Association configured to use
                combined_confidentiality_and_integrity_algorithms
     }
ensure that
     { when { IUT is requested to send first 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 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_02		
Summary:	Test of generating subsequent unicast IPv6 packets with ESP Header, tunnel mode		
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		
IUT Role	Ipsec_host	Test Case:	TC_SEC_3108_02
•	T and destination_node		Security_Association
and ES	P_Security_Association		
	combined_confidential	.ity_and_integrity_algo:	rithms
}			
ensure that			
{ when {	IUT is requested to se		et in tunnel_mode
+1 (containing ESP_Hea	,	
tnen {	IUT sends IPv6Packet i		boods.
	set to 50	eader_field of previous	_neader
	and containing (ESP He	and an	
	5 \ <u>=</u>	ader . ning Security Paramete:	ra Indox
		et to Security_Paramete:	_
	56	received from des	
		during SA_establis	_
	and contai	.ning sequence_number se	
		ence_number of previous	
	-	ning necessary padding	_
		.ning pad_length	
	set to number of padding_bytes		
	and containing correctly calculated		
		Integrity_Check_Va	lue
	includ	ling necessary padding_l	_
}			,

A.3 Key Exchange (IKEv2) Protocol

A.3.1 Exchange Message Structures

```
Test Purpose
Identifier:
                TP_SEC_6400_01
Summary:
               Test of generating IKE_SA_INIT request
               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,
References:
               RQ_002_6263, RQ_002_6304, RQ_002_6344
IUT Role
               Host
                                          Test Case:
                                                                    TC_SEC_6400_01
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
                     containing (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
              RQ 002 6401, RQ 002 6036, RQ 002 6232, RQ 002 6233, RQ 002 6236, RQ 002 6240,
References:
              RQ_002_6250, RQ_002_6263, RQ_002_6304, RQ_002_6344
IUT Role
              Host
                                     Test Case:
                                                              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 01
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_6232,
              RQ_002_6233, RQ_002_6236, RQ_002_6240, RQ_002_6250, RQ_002_6263, RQ_002_6310,
              RQ_002_6430, RQ_002_6431
IUT Role
                                      Test Case:
                                                               TC_SEC_6403_01
              Host
            IUT having sent IKE SA INIT request
with {
       and IUT having received IKE SA INIT response
ensure that
     { when { IUT is requested to send IKE_AUTH_request }
       then { IUT sends IKE_AUTH_request
                   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
                                           received 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 00010000'B'
                           and containing Message_ID set to 1)
              and containing (Encrypted_payload
                               containing Identification_payload_initiator
                                          'Next Payload field of previous
                                           payload is set to 35'
                           and containing Authentication_payload
                           and containing(Security_Association_payload
                                           containing at least 1 proposal
                                                containing at least 1 transform)
                           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 6405 01
              Test reaction on IKE AUTH request
Summary:
              RQ 002 6405, RQ 002 6036, RQ 002 6232, RQ 002 6233, RQ 002 6236, RQ 002 6240,
References:
              RQ_002_6250, RQ_002_6263, RQ_002_6312, RQ_002_6430, RQ_002_6431
                                                              TC_SEC_6405_01
IUT Role
                                     Test Case:
              Host
with {
          IUT having received IKE_SA_INIT_request
      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
              Test of generating CREATE_CHILD_SA request
Summary:
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
                                      Test Case:
IUT Role
                                                               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
References:
              RQ 002 6409, RQ 002 6036, 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_6409_01
              Host
with {
           IUT having completed IKE_SA_INIT exchange
       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
              TP SEC 6411 01
Identifier:
              Test of generating INFORMATIONAL_request
Summary:
              RQ 002 6411, RQ 002 6035, RQ 002 6232, RQ 002 6233, RQ 002 6236, RQ 002 6240,
References:
              RQ_002_6250
IUT Role
                                      Test Case:
                                                             TC_SEC_6411_01
              Host
with { IUT having established an IKE_Security_Association
ensure that
     { when { IUT is requested to send INFORMATIONAL_request }
       then { IUT sends INFORMATIONAL_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_request
                           and containing Major_Version set to 2
                           and containing Exchange_Type set to 37 INFORMATIONAL
                           and containing Flags set to 00010000'B'
                           and containing Message_ID
                                    set to previous sent Message_ID plus 1)
              and containing (Encrypted_payload
                               containing 0 or more Notify_payload
                           and containing 0 or more Delete_payload
                           and containing 0 or more Configuration_payload) }
```

```
Test Purpose
Identifier:
              TP_SEC_6412_01
              Test reaction on INFORMATIONAL_request
Summary:
References:
              RQ_002_6412, RQ_002_6036, RQ_002_6232, RQ_002_6233, RQ_002_6236, RQ_002_6240,
              RQ_002_6250
                                                             TC_SEC_6412_01
IUT Role
              Host
                                     Test Case:
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
                                       Test Case:
                                                                TC_SEC_6468_01
IUT Role
              Host
with {
       IUT having established an IKE_Security_Association
ensure that
     { when {
                  IUT receives INFORMATIONAL_request
                       containing (Configuration_payload
                                    containing Configuration_Type
                                        set to 1 CFG_REQUEST
                               and containing any unsupported
                                                Configuration Attribute) }
       then {
                  IUT sends INFORMATIONAL_response
                       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
               Test reaction on INFORMATIONAL_request containing incorrect value
Summary:
               RQ_002_6365, RQ_002_6368
References:
                                                                  TC_SEC_6365_01
               Host
                                        Test Case:
with {
       IUT having established an IKE_Security_Association
ensure that
     { when { IUT receives INFORMATIONAL_request
                    containing 'syntactically incorrect value' }
       then { IUT sends INFORMATIONAL_response
                    containing (Encrypted_payload
                                 containing Notify_payload
                                             containing Notify_Message_Type
                                                  set to 7 INVALID_SYNTAX) }
```

```
Test Purpose
Identifier:
               TP SEC 6375 01
Summary:
               Test reaction on CREATE_CHILD_SA request containing Traffic Selectors indicating address range
References:
               RQ_002_6375
IUT Role
                                       Test Case:
                                                                TC_SEC_6375_01
              Host
            IUT having established an IKE_Security_Association
with {
       and IUT 'only supporting Traffic Selectors specifying a
                 single pair of addresses'
     }
ensure that
     { when { IUT receives CREATE_CHILD_SA_request
                   containing (Traffic_Selector_payload
                                 containing Traffic_Selector
                                     indicating 'address range') }
       then { IUT sends CREATE_CHILD_SA_response
                   containing (Notify_payload
                                containing Notify_Message_Type
                                     set to 34 SINGLE_PAIR_REQUIRED) }
```

		Test Purpose	
Identifier:	TP_SEC_6376_01		
Summary:	Test reaction on CREATE_CHIL	D_SA request when no mo	ore CHILD_SA can be established
References:	RQ_002_6376		
IUT Role	Host	Test Case:	TC_SEC_6376_01
with { II	JT having established ar	n IKE_Security_Ass	ociation
and IU	JT 'unable to establish	any further CHILD)_SA'
}			
ensure that			
{ when {	{ when { IUT receives CREATE_CHILD_SA_request }		
then {	,		
	containing (Notify_payload		
	containing Notify_Message_Type		
	set to 35 NO ADDITIONAL SAS) }		
}			•

```
Test Purpose
Identifier:
               TP_SEC_6379_01
Summary:
               Test reaction on CREATE_CHILD_SA request containing unacceptable Traffic Selectors
References:
               RQ_002_6379
IUT Role
              Host
                                        Test Case:
                                                                 TC_SEC_6379_01
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
                    containing (Notify_payload
                                 containing Notify_Message_Type
                                     set to 38 TS_UNACCEPTABLE) }
```

```
Test Purpose
Identifier:
               TP SEC 6393 01
Summary:
               Test reaction on CREATE_CHILD_SA request containing transport mode request
References:
               RQ 002 6393
IUT Role
                                       Test Case:
              Host
                                                                TC_SEC_6393_01
            IUT having established an IKE_Security_Association
with {
       and IUT 'ready to accept transport mode request'
ensure that
     { when { IUT receives CREATE_CHILD_SA_request
                   containing (Notify_payload
                                containing Notify_Message_Type
                                     set to 16391 USE_TRANSPORT_MODE) }
       then { IUT sends CREATE_CHILD_SA_response
                   containing (Notify_payload
                                 containing Notify_Message_Type
                                     set to 16391 USE TRANSPORT MODE) }
```

```
Test Purpose
Identifier:
               TP_SEC_6394_01
               Test reaction on CREATE_CHILD_SA request containing transport mode request
Summary:
References:
               RQ_002_6394
IUT Role
              Host
                                        Test Case:
                                                                 TC_SEC_6394_01
with {
            IUT having established an IKE_Security_Association
       and IUT 'not ready to accept transport mode request'
ensure that
     { when { IUT receives CREATE_CHILD_SA_request
                    containing (Notify_payload
                                 containing Notify_Message_Type
                                     set to 16391 USE_TRANSPORT_MODE) }
       then { IUT sends CREATE_CHILD_SA_response
               not containing (Notify_payload
                                 containing 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
                                         Test Case:
                                                                   TC SEC 6007 01
IUT Role
               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:
              RQ 002 6014, RQ 002 6016, RQ 002 6062, RQ 002 6064, RQ 002 6415,RQ 002 6416,
References:
              RQ_002_6417
                                    Test Case:
IUT Role
             Host
                                                           TC_SEC_6014_01
with {
           IUT having established an IKE_Security_Association
ensure that
     { when { IUT is requested to send INFORMATIONAL_request
                  containing Delete_payload }
       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:	ummary: 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		
with {	TT having established an IKE_Security_Association		
and IU	TT having established at least 1 CHILD_SA		
}			
ensure that			
{ when {	IUT is requested to send INFORMATIONAL_request		
,	<pre>containing Delete payload }</pre>		
then {	IUT sends INFORMATIONAL_request		
	containing IKE Header		
	and containing (Encrypted_payload		
	containing Delete payload		
	containing Protocol ID indicating 2 or		
3	3 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
Summary:
               Test of generating IKE_AUTH request for extensible authentication methods, message 3
References:
               RQ_002_6151
IUT Role
                                         Test Case:
                                                                   TC_SEC_6151_01
               Host
with { ordered (
                       IUT having sent IKE_SA_INIT_request
                   and IUT having received IKE_SA_INIT_response )
        and IUT configured 'to use extensible authentication methods'
ensure that
     { when { IUT is requested to send IKE_AUTH_request }
        then { IUT sends IKE_AUTH_request
               not containing Authentication_payload }
```

		Test Purpose	
Identifier:	Identifier: TP_SEC_6152_01		
Summary:	Test reaction on IKE_AUTH requ	est for extensible authentication me	ethods, message 3
References:	RQ_002_6152, RQ_002_6153		
IUT Role	Host	Test Case:	TC_SEC_6152_01
with { ordere	ed (IUT having rece	eived IKE_SA_INIT_reques	st
	and IUT having sent	: IKE_SA_INIT_response)	1
and IU	JT configured 'to suppor	rt extensible authentica	ation methods'
}			
ensure that			
$\{$ when $\{$	IUT receives IKE_A	AUTH_request	
	not containing Aut	chentication_payload }	
then {	then { IUT sends IKE_AUTH_response		
	containing Ext	ensible_Authentication_	_Protocolpayload
	and containing Identification payload		
	and containing Authentication_payload		
	and not containing Security_Association_payload		pad
	and not containing any	Traffic_Selector_paylo	oad }
}			,

```
Test Purpose
Identifier:
               TP_SEC_6153_01
Summary:
               Test of generating IKE_AUTH request for extensible authentication methods, message 5
References:
               RQ_002_6153
IUT Role
                                       Test Case:
                                                                 TC_SEC_6153_01
              Host
with { ordered (
                       IUT having sent IKE_SA_INIT_request
                                                                      'message 1'
                  and IUT having received IKE_SA_INIT_response
                                                                      'message 2'
                  and IUT having sent IKE AUTH request
                                                                      'message 3'
                  and IUT having received IKE AUTH response
                                                                      'message 4')
       and IUT configured 'to use extensible authentication'
     }
ensure that
     { when { IUT is requested to send IKE_AUTH_request }
       then { IUT sends IKE_AUTH_request
                   containing Extensible_Authentication_Protocol_payload }
```

```
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
                                      Test Case:
                                                               TC_SEC_6161_01
              Host
with { ordered (
                      IUT having received IKE_SA_INIT_request 'message 1'
                                                                   'message 2'
                  and IUT having sent IKE_SA_INIT_response
                  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			
Identifier:	TP_SEC_6162_01				
Summary:	Summary: Test reaction on IKE_AUTH request for extensible authentication methods, message 5				
References:	RQ_002_6162, RQ_002_6374				
IUT Role	Host	Test Case:	TC_SEC_6162_01		
with { ordere	ed (IUT having rece	eived IKE_SA_INIT_reques	st 'message 1'		
	and IUT having sent	t IKE_SA_INIT_response	'message 2'		
	and IUT having rece	eived IKE_AUTH_request	'message 3'		
	and IUT sent IKE_AU	TTH_response	'message 4')		
and I	JT having completed 'aut	thentication method unsu	ccessfully'		
}					
ensure that	ensure that				
{ when {	{ when { IUT receives IKE_AUTH_request				
	containing Extensi	ible_Authentication_Prot	cocol_payload }		
then	then { IUT sends IKE_AUTH_response				
containing (Notify_payload					
	containing Notify_Message_Type				
	se	et to 24 AUTHENTICATION_	_FAILED) }		
}			-		

```
Test Purpose
Identifier:
              TP_SEC_6164_01
Summary:
              Test of generating IKE_AUTH request for extensible authentication methods, message 7
References:
              RQ_002_6164
IUT Role
              Host
                                      Test Case:
                                                               TC_SEC_6164_01
with { ordered (
                      IUT having sent IKE_SA_INIT_request
                                                                     'message 1'
                  and IUT having received IKE_SA_INIT_response
                                                                     'message 2'
                  and IUT having sent IKE_AUTH_request
                                                                     'message 3'
                  and IUT having received IKE_AUTH response
                                                                     'message 4'
                  and IUT having sent IKE_AUTH_request
                                                                     'message 5'
                  and IUT having received IKE_AUTH_response
                                                                     'message 6' )
       and IUT 'ready to finalize extensible authentication'
ensure that
     { when { IUT is requested to send IKE_AUTH_request }
       then { IUT sends IKE_AUTH_request
                   containing Authentication_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
                                      Test Case:
             Host
                                                              TC_SEC_6164_02
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 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

		Test Purpose	
Identifier:	TP_SEC_6186_01		
Summary:	Test reaction on bad	ly formatted IKE_SA_INIT request	
References:	RQ_002_6186		
IUT Role	Host	Test Case:	TC_SEC_6186_01
with {	IUT ready to rec	eive IKE_SA_INIT_request	
and	I IUT ready to send	d IKE_SA_INIT response	
}			
ensure tha	t		
{ whe	n { IUT receives l	badly formatted IKE_SA_IN	IT request }
the	1	SA INIT response	,
	-	g Notify_payload }	
}		2 - 1 - 1 - 1 - 1 - 1 - 1 - 1	

```
Test Purpose
               TP_SEC_6186_02
Identifier:
               Test reaction on badly formatted IKE_AUTH request
Summary:
References:
               RQ_002_6186
               Host
IUT Role
                                        Test Case:
                                                                 TC_SEC_6186_02
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_01				
Summary:	Test reaction on badly formatted	IKE_SA_INIT response		
References:	RQ_002_6188			
IUT Role	Host	Test Case:	TC_SEC_6188_01	
<pre>with { IUT ha } ensure that { when { then { } }</pre>	<pre>with { IUT having sent IKE_SA_INIT_request } ensure that { when { IUT receives badly formatted IKE_SA_INIT_response }</pre>			

Test Purpose				
Identifier:	TP_SEC_6188_02			
Summary:	Test reaction on badly formatted IKE_AUTH respon	nse		
References:	RQ_002_6188			
IUT Role	Host Test Case:	TC_SEC_6188_02		
with { ordere	d (IUT having sent IKE_SA_INIT	T_request		
	and IUT having received IKE_SA_	_INIT_response		
	<pre>and IUT having sent IKE_AUTH_request)</pre>			
ensure that				
{ when { then {	<pre>IUT receives badly formatted IKE_A IUT sends no response }</pre>	AUTH_response }		

```
Test Purpose
              TP_SEC_6189_01
Identifier:
              Test reaction on request outside of known IKE_SA
Summary:
              RQ_002_6189, RQ_002_6190, RQ_002_6191
References:
                                                             TC_SEC_6189_01
IUT Role
             Host
                                      Test Case:
with { IUT having no IKE_Security_Association
ensure that
     { when { IUT receives CREATE_CHILD_SA_request on UDP_port_500 }
       then { IUT sends CREATE_CHILD_SA_response on UDP_port_500
                   containing destination_address
                       set to source_address
                              received in CREATE_CHILD_SA_request
              and containing (IKE_Header
                               containing IKE_SA_Initiators_SPI
                                   set to IKE_SA_Initiators_SPI
                                           received in CREATE_CHILD_SA_request
                           and containing IKE_SA_Responders_SPI
                                   set to IKE_SA_Responders_SPI
                                           received in CREATE_CHILD_SA_request
                           and containing Message_ID
                                   set to Message_ID
                                           received in CREATE_CHILD_SA_request)
              and not containing an Encrypted_payload
              and containing (Notify_payload -- Not encrypted
                               containing Notify_Message_Type
                                   set to 4 INVALID_IKE_SPI ) }
```

```
Test Purpose
Identifier:
              TP SEC 6189 02
Summary:
              Test reaction on request outside of known IKE_SA
References:
              RQ_002_6189, RQ_002_6190, RQ_002_6191
IUT Role
                                                             TC_SEC_6189_02
             Host
                                     Test Case:
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) }
```

	Test Purpose				
Identifier:	TP_SEC_6023_01				
Summary:	Test reaction on cryptographicall	y unprotected response indicating	invalid SPI		
References:	RQ_002_6023, RQ_002_6194				
IUT Role	Host	Test Case:	TC_SEC_6023_01		
with { IUT ha	ving established an IKE	E_Security_Association			
}					
ensure that					
{ when {	IUT receives CREATE_CH	HILD SA response			
	containing (IKE_Header				
	_	ining unknown IKE_SA_In	itiators SPI		
	and containing unknown IKE SA Responders SPI)				
	and not containing an	Encrypted payload			
	_	y_payload Not en	ncrvpted		
	containing Notify Message Type				
	set to 4 INVALID IKE SPI) }				
then {	<pre>set to 4 INVALID_IKE_SPI) } then { IUT sends no response } }</pre>				

```
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
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 INF	ORMATIONAL_request with Notify p	payload without cryptographic protection		
References:	RQ_002_6023, RQ_	002_6022			
IUT Role	Host	Test Case:	TC_SEC_6023_03		
with { IUT ha	ving establish	ed an IKE_Security_Assoc:	iation		
}					
ensure that					
{ when {	IUT receives	INFORMATIONAL_request			
,	not containing an Encrypted payload				
	containin	g (Notify_payload	- Not encrypted		
	containing Notify_Message_Type				
	<pre>set to 4 INVALID_IKE_SPI) }</pre>				
then {	then { IUT sends no INFORMATIONAL response }				
}		,			

A.3.4.3 General Protocol Handling

A.3.4.3.1 Address and Port Agility

```
Test Purpose
               TP_SEC_6206_01
Identifier:
               Test reaction on IKE_SA_INIT request received on UDP port other than 500 or 4500
Summary:
References:
               RQ_002_6206, RQ_002_6131, RQ_002_6212
                                        Test Case:
                                                                   TC_SEC_6206_01
IUT Role
               Host
            IUT ready to receive IKE SA INIT request
with {
       and IUT ready to send IKE SA INIT response
ensure that
     { when { IUT receives IKE_SA_INIT_request not on UDP_port_500
                                                and not on UDP_port_4500 }
        then { IUT sends IKE_SA_INIT_response on 'UDP port on which request
                                                       was 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
IUT Role
              Host
                                      Test Case:
       IUT having established an IKE_Security_Association
with {
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
               TP_SEC_6369_01
Identifier:
              Test reaction on request with incorrect Message ID
Summary:
References:
              RQ_002_6369, RQ_002_6370
IUT Role
              Host
                                       Test Case:
                                                                 TC_SEC_6369_01
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
                   IUT receives INFORMATIONAL_request
     { when {
                        containing (IKE_Header
                                     containing Message_ID 'out of sequence' }
       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 on request when se	ent request is not answered	
References:	RQ_002_6041		
IUT Role	Host	Test Case:	TC_SEC_6041_01
with { IU	JT having established Ik	<pre>KE_Security_Association</pre>	
and IU	JT having sent CREATE_CH	HILD_SA_request	
and IUT not having received CREATE_CHILD_SA_response			
}			
ensure that			
{ when {	IUT receives CREATE_CH	HILD SA request }	
then	IUT sends CREATE_CHILI		
}			

```
Test Purpose
Identifier:
               TP_SEC_6041_02
Summary:
               Test reaction on request when sent request is not answered
References:
               RQ_002_6041
IUT Role
                                         Test Case:
                                                                  TC_SEC_6041_02
               Host
with {
            IUT having established an IKE Security Association
       and IUT having sent INFORMATIONAL_request
       and IUT not having received INFORMATIONAL_response
ensure that
     { when { IUT receives INFORMATIONAL_request }
        then { IUT sends INFORMATIONAL_response }
```

A.3.4.3.5 Request Internal Address

```
Test Purpose
Identifier:
              TP_SEC_6177_01
              Test reaction on IKE_AUTH request with Configuration Payload
Summary:
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 }
```

	Test Purpose				
Identifier:	TP_SEC_6184_01	•			
Summary:	Test reaction on IKE_AUTH	I request with Configuration	n Payload		
References:	RQ_002_6184, RQ_002_6	462			
IUT Role	lpsec_gateway	Test Case:	TC_SEC_6184_01		
with { IUT co	onfigured 'to expect	IKE_AUTH request	to include		
	the Confi	guration Payload'			
}					
ensure that					
{ when {	{ when { IUT receives IKE AUTH request				
not containing (Configuration_payload					
containing Configuration_Type					
set to 1 CFG REOUEST }					
then {	IUT sends IKE_AUTH	I response	_ ~ ,		
containing (Notify_payload					
containing Notify Message Type					
set to 37 FAILED CP REQUIRED) }					
}		JCC CC 57 TATHER			

A.3.4.3.6 Retransmission Timers

```
Test Purpose
Identifier:
              TP_SEC_6030_01
Summary:
              Test reaction on repeated IKE_SA_INIT request
References:
              RQ_002_6030, RQ_002_6046
IUT Role
                                      Test Case:
                                                               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		
Summary:	Test reaction on repeated IKE_AUTH request		
References:	RQ_002_6030, RQ_002_6046		
IUT Role	Host		
with { ordere	ed (IUT having received IKE_AUTH_request		
	and IUT having sent IKE_AUTH_response)		
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 }		

Test Purpose			
Identifier:	TP_SEC_6030_03		
Summary:	Test reaction on repeated CREAT	TE_CHILD_SA request	
References:	RQ_002_6030, RQ_002_6046		
IUT Role	Host	Test Case:	TC_SEC_6030_03
with { ordere	d (IUT having rece	eived CREATE_CHILD_SA_re	equest
	and IUT having sent	: CREATE_CHILD_SA_respor	nse)
ensure that { when { IUT receives previous CREATE_CHILD_SA_request i.e. the same as the one that it has already answered }			
$ ag{then } egin{cases} \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	IUT resends previous C	REATE_CHILD_SA_response	e }

```
Test Purpose
              TP_SEC_6030_04
Identifier:
              Test reaction on repeated INFORMATIONAL_request
Summary:
References:
              RQ_002_6030, RQ_002_6046
IUT Role
                                      Test Case:
                                                              TC_SEC_6030_04
              Host
with { ordered (
                      IUT having received INFORMATIONAL_request
                  and IUT having sent INFORMATIONAL_response)
ensure that
     { when { IUT receives previous INFORMATIONAL_request -- i.e. the same as
                                                                -- the one that it
                                                                -- has already
                                                                -- answered
       then {    IUT resends previous INFORMATIONAL_response }
```

	Test Purpose				
Identifier:	TP_SEC_6033_01				
Summary:	Test resending of unanswered IK	E_SA_INIT request			
References:	RQ_002_6033, RQ_002_6045				
IUT Role	Host	Test Case:	TC_SEC_6033_01		
<pre>with { IUT ha } ensure that { when { then { }</pre>	IVI receives no IKE_SA_INIT_R IUT receives no IKE_SA_INIT_R				

Test Purpose			
Identifier:	TP_SEC_6033_02		
Summary:	Test resending of unanswered IK	E_AUTH request	
References:	RQ_002_6033, RQ_002_6045		
IUT Role	Host	Test Case:	TC_SEC_6033_02
<pre>with { IUT ha } ensure that { when { then { } }</pre>	IVI receives no IKE_AUTH_required IUT receives no IKE_AUTH_INGLE IUT resends previous I	JTH_response }	

	Test Purpose				
Identifier:	TP_SEC_6033_03				
Summary:	Test resending of unanswered Cl	REATE_CHILD_SA request			
References:	RQ_002_6033, RQ_002_6045				
IUT Role	Host	Test Case:	TC_SEC_6033_03		
<pre>with { IUT ha } ensure that { when { then { } }</pre>	IUT receives no CREATE IUT resends previous (}		

A.3.4.3.7 Version Compatibility

```
Test Purpose
Identifier:
               TP_SEC_6065_01
               Test reaction on IKE_SA_INIT request with major version > 2
Summary:
               RQ_002_6065, RQ_002_6066, RQ_002_6237
References:
                                       Test Case:
                                                                 TC_SEC_6065_01
IUT Role
              Host
with {
       IUT ready to establish a Security_Association using IKEv2
ensure that
                   IUT receives IKE_SA_INIT_request
     { when {
                        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
Identifier:
               TP SEC 6065 02
Summary:
               Test reaction on IKE_AUTH request with major version > 2
References:
               RQ_002_6065, RQ_002_6066, RQ_002_6237
IUT Role
                                                                 TC_SEC_6065_02
              Host
                                        Test Case:
                       IUT having received IKE SA INIT request
with { ordered (
                  and IUT having sent IKE_SA_INIT_response)
ensure that
     { when {
                   IUT receives IKE_AUTH_request
                        containing (IKE_Header
                                     containing Major_Version
                                         set to greater than 2) }
                    IUT discards IKE_AUTH_request
       then {
               and optionally (
                    IUT sends IKE_AUTH_response
                        containing (Notify_payload
                                     containing Notify_Message_Type
                                         set to 5 INVALID_MAJOR_VERSION) }
```

```
Test Purpose
Identifier:
               TP SEC 6065 03
Summary:
               Test reaction on CREATE_CHILD_SA request with major version > 2
References:
              RQ_002_6065, RQ_002_6066, RQ_002_6237
                                                                 TC_SEC_6065_03
IUT Role
              Host
                                       Test Case:
with { IUT having established an IKE_Security_Association
ensure that
                   IUT receives CREATE_CHILD_SA_request
     { when {
                        containing (IKE_Header
                                     containing Major_Version
                                         set to greater than 2) }
       then {
                   IUT discards CREATE_CHILD_SA_request
               and optionally (
                   IUT sends CREATE_CHILD_SA_response
                        containing (Notify_payload
                                     containing Notify_Message_Type
                                         set to 5 INVALID_MAJOR_VERSION) }
```

Test Purpose				
Identifier:	TP_SEC_6065_04			
Summary:	Test reaction on INFORMATIONAL_request	with major version > 2		
References:	RQ_002_6065, RQ_002_6066, RQ_002_623	37		
IUT Role	Host Test Case	:	TC_SEC_6065_04	
with { IUT ha	ving established an IKE_Securit	y_Association		
}				
ensure that				
{ when {	IUT receives INFORMATIONAL	_request		
	containing (IKE_Header	:		
	containing Major Version			
	set to greater than 2 }			
then {	then { IUT discards INFORMATIONAL request			
	and optionally (
IUT sends INFORMATIONAL response				
containing (Notify payload				
containing 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
                                       Test Case:
                                                                TC_SEC_6068_01
IUT Role
              Host
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
              TP_SEC_6068_02
Identifier:
Summary:
              Test reaction on IKE_AUTH request with major version < 2
References:
              RQ_002_6068, RQ_002_6067, RQ_002_6069
IUT Role
                                      Test Case:
                                                                TC_SEC_6068_02
              Host
with { ordered (
                       IUT having sent IKE_SA_INIT_request
                  and IUT having received IKE_SA_INIT_response)
     }
ensure that
     { when { IUT receives IKE_AUTH_request
                   containing (IKE_Header
                                containing Major_Version set to 1) }
       then { IUT sends IKE_AUTH_response
                   containing (IKE_Header
                                containing Major_Version set to 1
                            and containing V_Bit set to 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, RQ_002_6069			
IUT Role	Host Test Case: TC_SEC_6068_03			
ensure that { when {	<pre>with { IUT having established an IKE_Security_Association }</pre>			
}	<pre>and containing V_Bit set to 1) }</pre>			

	Test Purpose
Identifier:	TP_SEC_6068_04
Summary:	Test reaction on INFORMATIONAL_request with major version < 2
References:	RQ_002_6068, RQ_002_6067, RQ_002_6069
IUT Role	Host Test Case: TC_SEC_6068_04
with { IUT ha	aving 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) }
```

	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			
with { IUT ha	aving established an IKE_Security_Association			
}				
ensure that				
{ when {	{ when { IUT receives INFORMATIONAL request			
containing unrecognized (payload				
<pre>containing C_Bit set to 1) }</pre>				
then { IUT sends INFORMATIONAL response				
containing (Notify_payload				
containing Notify_Message_Type				
set to 1 UNSUPPORTED CRITICAL PAYLOAD) }				
}				

Test Purpose				
Identifier:	TP_SEC_6073_01			
Summary:	Test reaction on CREATE_CHILI	D_SA request with unrecognized page	ayload	
References:	RQ_002_6073, RQ_002_6256			
IUT Role	Host	Test Case:	TC_SEC_6073_01	
with { IUT ha	ving established an IKE	_Security_Association		
}				
ensure that				
{ when {	{ when { IUT receives CREATE_CHILD_SA_request			
containing unrecognized (payload				
<pre>containing C_Bit set to 0) }</pre>				
then {	then { IUT sends CREATE_CHILD_SA_response			
not containing (Notify_payload				
containing Notify Message Type				
set to 1 UNSUPPORTED CRITICAL PAYLOAD) }				
}			,	

```
Test Purpose
Identifier:
               TP SEC 6073 02
Summary:
               Test reaction on INFORMATIONAL_request with unrecognized payload
References:
               RQ_002_6073, RQ_002_6256
IUT Role
                                        Test Case:
                                                                 TC_SEC_6073_02
              Host
with { IUT having established an IKE_Security_Association
ensure that
     { when { IUT receives INFORMATIONAL_request
                    containing unrecognized (payload
                                containing C_Bit set to 0) }
       then { IUT sends INFORMATIONAL_response
               not containing (Notify_payload
                                 containing Notify_Message_Type
                                     set to 1 UNSUPPORTED_CRITICAL_PAYLOAD) }
```

A.3.4.4 Security Parameter Negotiation

A.3.4.4.1 Algorithm Negotiation

Test Purpose			
Identifier:	TP_SEC_6088_01		
Summary:	Test reaction on IKE_SA_INIT request with several SA proposal		
References:	RQ_002_6088, RQ_002_6271		
IUT Role	Host T	est Case:	TC_SEC_6088_01
ensure that { when {	contain: [IUT sends IKE_SA_INIT_recontaining (Security)	T_request y_Association_payload ing at least 1 accept	able Proposal) }
}		-	

```
Test Purpose
Identifier:
               TP SEC 6088 02
Summary:
               Test reaction on IKE_AUTH request with several SA proposal
References:
               RQ_002_6088, RQ_002_6271
IUT Role
                                        Test Case:
                                                                  TC_SEC_6088_02
               Host
            IUT having sent IKE SA INIT request
with {
       and IUT having received IKE SA INIT response
ensure that
     { when { IUT receives IKE AUTH request
                    containing (Security_Association_payload
                                 containing at least 1 acceptable Proposal) }
       then { IUT sends IKE_AUTH_response
                    containing (Security_Association_payload
                                 containing 1 Proposal) }
```

```
Test Purpose
              TP_SEC_6088_03
Identifier:
              Test reaction on CREATE_CHILD_SA request with several SA proposal
Summary:
References:
              RQ_002_6088, RQ_002_6271
IUT Role
                                       Test Case:
                                                                TC_SEC_6088_03
              Host
with { IUT having established an IKE_Security_Association
ensure that
     { when { IUT receives CREATE_CHILD_SA_request
                   containing (Security_Association_payload
                                containing at least 1 acceptable Proposal) }
       then { IUT sends CREATE_CHILD_SA_response
                   containing (Security_Association_payload
                                containing 1 Proposal) }
```

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	Host	Test Case:	TC_SEC_6372_01
with { IUT re	eady to establish a Secu	rity_Association using	IKEv2
}			
ensure that			
{ when {	{ 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			
Summary:	Test reaction on IKE_AUTH request with unacceptable SA proposal			
References:	RQ_002_6372			
IUT Role	Host	Test Case:	TC_SEC_6372_02	
with { II	JT having sent IKE_SA_IN	IT_request		
and IU	JT having received IKE_S	A_INIT_response		
}				
ensure that				
{ when {	{ IUT receives IKE_AUTH_	request		
containing (Security_Association_payload				
containing no acceptable Proposal) }				
then { IUT sends IKE AUTH response				
containing (Notify payload				
containing Notify Message Type				
set to 14 NO PROPOSAL CHOSEN) }			OSEN) }	
}			. ,	

```
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
with { IUT having established an IKE_Security_Association
ensure that
     { when { IUT receives CREATE_CHILD_SA_request
                    containing (Security_Association_payload
                                 containing no acceptable Proposal) }
       then { IUT sends CREATE_CHILD_SA_response
                    containing (Notify_payload
                                 containing Notify_Message_Type
                                     set to 14 NO_PROPOSAL_CHOSEN) }
```

```
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
               Host
                                        Test Case:
                                                                  TC_SEC_6373_01
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
              Test reaction on IKE_SA_INIT response with COOKIE Notify payload
Summary:
References:
              RQ_002_6081, RQ_002_6080, RQ_002_6391
                                                                TC_SEC_6081_01
IUT Role
              Host
                                       Test Case:
       IUT having sent IKE_SA_INIT_request
with {
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
                                                                 TC_SEC_6101_01
IUT Role
              Host
                                       Test Case:
            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
                 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	Host	Test Case:	TC_SEC_6102_01
with { IU	${f T}$ having established ar	IKE_Security_Associate	ion
and IU	T having established a	CHILD_SA	
and IU	$^{ m T}$ 'having detected that	the lifetime of the CF	HILD_SA
	was about to expire'		
and IU	T having sent CREATE CH	HILD_SA_request 'for re	keying'
}] }		
ensure that			
{ when {			
then	,		
containing (Delete payload			
containing Security Parameters Index			
<pre>indicating CHILD_SA 'to be deleted') }</pre>			
}	Indice	citing chilib_ba to be de	zicca , j

		Test Purpose		
Identifier:	TP_SEC_6103_01			
Summary:	Test of generating CREATE_CH	Test of generating CREATE_CHILD_SA request for rekeying of IKE SA		
References:	RQ_002_6103			
IUT Role	Host	Test Case:	TC_SEC_6103_01	
with {	UT having established a	n IKE_Security_Associat:	ion	
and I	UT having established a	CHILD_SA		
and I	UT 'having detected tha	t the lifetime of the II	KE_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				
<pre>and not containing Traffic_Selector_payload_responder }</pre>				
}	3		,	

```
Test Purpose
Identifier:
              TP_SEC_6105_01
              Test of deletion of old IKE_SA after rekeying
Summary:
References:
              RQ_002_6105
IUT Role
                                      Test Case:
                                                               TC_SEC_6105_01
             Host
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				
Identifier:	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			TC_SEC_6123_01
with { IUT ha	ving	established an IKE	_Security_Association	
}				
ensure that				
$\{$ when $\{$	IUT	receives CREATE_CH	IILD_SA_request	
		containing (Traffi	.c_Selector_payload_in:	itiator
		contai	ning first	
			and acceptable Traff:	ic_Selector
		and contai	ning next	
			and unacceptable Traf:	fic_Selector)
	and containing (Traffic_Selector_payload_responder			
		contai	ning first	
	and acceptable Traffic_Selector			
		and contai	ning next	
	<pre>and unacceptable Traffic_Selector) }</pre>			fic_Selector) }
then {	IUT	sends CREATE_CHILD	_SA_response	·
		containing (Traffi	c_Selector_payload_in:	itiator
		contai	ning acceptable Traff:	ic_Selector
		rece	ived in CREATE_CHILD_S	SA_request)
	and	containing (Traffi	.c_Selector_payload_res	sponder
			ning acceptable Traff:	
			ived in CREATE_CHILD_S	
}			_	-

```
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
                                      Test Case:
IUT Role
              Host
                                                              TC_SEC_6125_01
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		