ETSI TS 102 624-2 V1.1.1 (2008-10)

Technical Specification

Broadband Radio Access Networks (BRAN);
HiperMAN;
Conformance Testing for the Network layer of the HiperMAN/WiMAX terminal devices;
Part 2: Test Suite Structure and Test Purposes (TSS&TP)

Reference

DTS/BRAN-004T009-2

Keywords

HiperMAN, layer 3, terminal, testing, TSS&TP

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

Copyright Notification

Contents

Intellectual Property Rights 4

Foreword....4

1 Scope 5

2 References 5
2.1 Normative references 5
2.2 Informative references....7

3 Definitions and abbreviations....7
3.1 Definitions....7
3.2 Abbreviations 7

4 Test Suite Structure (TSS)....8
4.1 Structure 8
4.2 Test groups 9
4.2.1 Protocol services....9
4.2.2 Main test types....9
4.2.2.1 Valid Behaviour (BV) tests....9
4.2.2.2 Invalid Behaviour (BI) tests 9
4.2.2.3 Inopportune Behaviour (BO) tests 9
4.2.2.4 Timer and counter (TI) tests....9

5 Test Purposes (TP) 9
5.1 Introduction....9
5.1.1 TP definition conventions....9
5.1.2 TP Identifier naming conventions....10
5.1.3 Sources of TP definitions....10
5.1.4 TP selection criteria name convention....10
5.2 Test purposes for MS 11
5.2.1 Network selection and entry 11
5.2.2 DHCP group 11
5.2.2.1 DHCP timer....14
5.2.3 CMIPv4 15
5.2.4 QoS 18
5.2.5 Security....19
5.2.5.1 Device authentication....19
5.2.5.1.1 Retry behaviour 21
5.2.5.1.2 Fragmentation....21
5.2.5.2 User authentication....22
5.2.5.2.1 EAP-AKA 22
5.2.5.2.2 EAP-TTLS....24
5.2.5.3 CMAC Keys....27
5.2.6 IPv6....28
5.2.7 CMIPv6 29

Annex A (informative): Bibliography....34

History 35

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 Broadband Radio Access Networks (BRAN).

1 Scope

The present document contains the Test Suite Structure (TSS) and Test Purposes (TP) to test the HiperMAN/WiMAX terminals based on the WiMAX Forum Network Architecture specifications.

The objective of the present document is to provide a basis for conformance tests for WiMAX terminal equipment giving a high probability of air interface inter-operability between different manufacturers' WiMAX equipment.

The ISO standard for the methodology of conformance testing (ISO/IEC 9646-1 [21] and ISO/IEC 9646-2 [22]) as well as the ETSI rules for conformance testing (ETS 300 406 [20]) are used as a basis for the test methodology.

2 References

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

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

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

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

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

2.1 Normative references

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

[1] WiMAX Forum (V1.2.1): "WiMAX Forum Network Architecture; Stage 1: Architecture Tenets, Reference Model and Reference Points, Part 1".

NOTE: Available at http://www.wimaxforum.org/technology/documents/WiMAX_Forum_Network_Architecture_Stage_2-3_Rel_1v1.2.zip.

[2] WiMAX Forum (V1.2.1): "WiMAX Forum Network Architecture, Stage 2: Architecture Tenets, Reference Model and Reference Points, Part 2".

NOTE: Available at http://www.wimaxforum.org/technology/documents/WiMAX_Forum_Network_Architecture_Stage_2-3_Rel_1v1.2.zip.

[3] WiMAX Forum (V1.2.1): "WiMAX Forum Network Architecture, Stage 3: Detailed Protocols and Procedures".

NOTE: Available at http://www.wimaxforum.org/technology/documents/WiMAX_Forum_Network_Architecture_Stage_2-3_Rel_1v1.2.zip.

[4] ETSI TS 102 624-1: "Broadband Radio Access Networks (BRAN); HiperMAN; Conformance Testing for the Network Layer of HiperMAN/WiMAX terminal devices; Part 1: Protocol Implementation Conformance Statement (PICS) proforma".

[5] IEEE 802.16e-2005: "IEEE Standard for Local and metropolitan area networks - Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems. Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1".

NOTE: Available at http://standards.ieee.org/getieee802/802.16.html.

[6] IETF RFC 1256 (September 1991): "ICMP Router Discovery Messages ".

[7] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[8] IETF RFC 2131 (March 1997): "Dynamic Host Configuration Protocol".

[9] IETF RFC 2132 (March 1997): "DHCP Options and BOOTP Vendor Extensions".

[10] IETF RFC 3344 (August 2002): "IP Mobility Support for IPv4".

[11] IETF RFC 4187 (January 2006): "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[12] IETF RFC 5281: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)".

[13] IETF RFC 3748 (June 2004): "Extensible Authentication Protocol (EAP)".

[14] IETF RFC 4861: "Neighbor Discovery for IP version 6 (IPv6)".

[15] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[16] IETF RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[17] IETF RFC 3775 (June 2004): "Mobility Support in IPv6".

[18] IETF RFC 4285 (January 2006): "Authentication Protocol for Mobile IPv6".

[19] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

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

[21] ISO/IEC 9646-1 (1994): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 1: General concepts". (See also ITU-T Recommendation X.290 (1991).

[22] ISO/IEC 9646-2 (1994): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 2: Abstract Test Suite specification". (See also ITU-T Recommendation X.291 (1991).

[23] ISO/IEC 9646-6 (1994): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 6: Protocol profile test specification".

[24] ISO/IEC 9646-7 (1995): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statement".

[25]	ETSI TS 155 205: "Digital cellular telecommunications system (Phase 2+); Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8 (3GPP TS 55.205 version 7.0.0 Release 7)".

2.2 Informative references

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

Not applicable.

[i.1]	ETSI TS 102 178: "Broadband Radio Access Networks (BRAN); HiperMAN; Data Link Control (DLC) layer".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ISO/IEC 9646-7 [24], TS 102 178 [i.1] and IEEE 802.16e-2005 [5] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ISO/IEC 9646-1 [21], ISO/IEC 9646-6 [23], ISO/IEC 9646-7 [24], TS 102 178 [i.1], IEEE 802.16e-2005 [5] and the following apply:

AKA	Authentication and Key Agreement
AVP	Attribute Value Pair
BO	Inopportune Behaviour
BS	Base Station
BU	Binding Update
BV	Valid Behaviour
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
EAP	Extensible Authentication Protocol
FQDN	Fully Qualified Domain Name
IP	Internet Protocol
ISF	Initial Service Flow
IUT	Implementation Under Test
MAC	Medium Access Control
MS	Mobile Station
NAI	Network Access Identifier
NAP	Network Access Provider
NSP	Network Service Provider
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
QoS	Quality of Service
TE	Test Equipment
TE	Test Equipment
TI	Timer
TLS	Transport Layer Security
TP	Test Purposes
TSS	Test Suite Structure
TTLS	Tunneled Transport Layer Security
UL	UplinkBI Invalid Behaviour

4 Test Suite Structure (TSS)

4.1 Structure

Figure 1 shows the DLC Test Suite Structure (TSS) including its subgroups defined for conformance testing.

Group	Function	Sub-function
Network Entry (4.1)		
	Network Discovery (4.1.2)	
	Network Selection/re-selection 4.1.2)	
Addressing		
	CMIPv4	
		MS Registration
		MS Re-registration
		Session Termination
		CSN anchor mobility
	CMIPv6	
		MS Registration
		Inter-access Router Handover
		Session Renewal
		Session Termination
	IPv6 Stateless address management	
		Router Solicitation
		Without Router Solicitation
Client DHCPv4		
	Discover	
	Request-Response	
	Use of DHCP allocated IP address	
	DHCP Renew	
Security		
	Device authentication (4.4.1.2.1 stg3)	
		EAP-TLS
	User authentication	
		EAP-AKA
		EAP-TTLS
	EAP-AKA	
	EAP-TTLSv0/MS-CHAP-v02	
		Certificate Request
		Without Certificate Request
Network Entry and Exit		
	Nwk Entry - Single EAP (4.5.1.1)	
	Nwk Entry - Double EAP (4.5.1.2)	
	Nwk Exit – Normal mode (4.5.2.1)	
	Nwk Exit – Idle mode (4.5.2.2)	
Mobility (CSN anchored) 4.8		
	Client MIP4 (4.8.3)	
	Client MIP6 (4.8.4)	
IPv6		

Figure 1: TSS for WiMAX Forum Network architecture

The test suite is structured as a tree with the root defined as DLC-BS or DLC-MS representing the protocol groups "DLC for BS" or "DLC for MS". The tree is of rank 3 with the first rank a Group, the second a Function, and the third a sub-function. The third rank is broken down into the standard ISO conformance test categories CA, BV, BI, BO and TI (discussed below).

NOTE: For compatibility with TP identifier names in earlier releases of the HiperMAN DLC Test Purposes document, the protocol group "DLC for MS" in the present document is still denoted "SS".

4.2 Test groups

Each test group has a total of three levels. The first level is the protocol services. The second level separates the protocol services into the various functional areas. The third level are the sub-functional areas. The fourth level, if required, is used to indicate the initiator (BS or MS) or the direction of communication (DL or UL). This fourth level is not shown in figure 1.

4.2.1 Protocol services

To be added in the next release.

4.2.2 Main test types

The main test types are the valid behaviour group, the invalid behaviour group and the inopportune behaviour group.

4.2.2.1 Valid Behaviour (BV) tests

This test group shall verify that the IUT reacts in conformity with the base specifications after receipt or exchange of valid Protocol Data Units (PDUs). Valid PDUs means that the exchange of messages and the content of the exchanged messages are considered as valid.

4.2.2.2 Invalid Behaviour (BI) tests

This test sub group shall verify that the IUT reacts in conformity with the base specifications after receipt of a syntactically invalid PDU.

4.2.2.3 Inopportune Behaviour (BO) tests

This test sub group shall verify that the IUT reacts in conformity with the base specifications after receipt of a syntactically correct PDU not expected in the actual message exchange.

4.2.2.4 Timer and counter (TI) tests

This test group shall verify that the IUT reacts in conformity with the base specifications after expiry of a defined timer or counter.

5 Test Purposes (TP)

5.1 Introduction

5.1.1 TP definition conventions

The TPs are defined by the rules shown in table 1.

Table 1: TP definition rules

TP Definition Item	Item Description
TP Id	The TP Id is a unique identifier formed according to the TP naming conventions defined in the clause below.
WiMAX Forum Nwrk Architecture Reference	A pointer to the base specification requirement from which the TP is derived (specification reference, clause and paragraph).
PICS Item	The PICS item(s) associated with this TP.
Initial Condition	The IUT's state to which the TP is applied.
Expected behaviour	Definition of the events that are expected from the IUT pursuant to the base specification given a certain stimulus.
Notes	Additional optional information provided to the TP reader.

5.1.2 TP Identifier naming conventions

The identifier of the TP is built according to table 2.

Table 2: TP naming convention

Identifier	TP/<pg>/<fg>/<sg>/<x>-H<nnn>		
	<st> = side type	MS	Mobile Station
	<pg> = protocol group	CMIPv4	Client Mobile IP v4
		DHCP	Dynamic Host Configuration Protocol
		QoS	Quality of Service
		SEC	Security
		IPv6	IP v6
		CMIPv6	Client Mobile IP v6
	<fg> = function group		To be added in subsequent releases
	<sg> = subfunction group		To be added in subsequent releases
	<x> = type of testing		To be added in subsequent releases
	<nnn> = sequential number	Hnnn	(H000, H001, etc.)

5.1.3 Sources of TP definitions

All TPs are specified according to WiMAX Forum Network Architecture Stage 2, and 3 documents [1], [2] and [3].

5.1.4 TP selection criteria name convention

The mapping relationship between selection criteria of the TP and answer items of PICS is listed in table 3.

Table 3: TP Selection Criteria name convention

Identifier	Selection Criteria in TP	Answer Items in PICS	Criteria
1	PIC_CMIPV4	Ax.x [x]	MS supports CMIPv4 for address assignment
2	PIC_EAPAKA	Ay.y [x]	MS supports EAP-AKA user authentication.
3	PIC_EAPTTLS	Ay.y [x]	MS supports EAP-TTLS user authentication.
4	PIC_DHCPv4	A.2/1 [4]	MS supports DHCPv4
5	PIC_CMIPV4	A.2/2	MS supports CMIPv4
6			
7			
8			
9			
10			
11			
12			
13			

5.2 Test purposes for MS

5.2.1 Network selection and entry

TP ID	TP/MS/NWE/BV-H000
Reference	WFNA Stage3 [3]: section 4.1.2.3.1.
PICS Item	
Initial Condition	The IUT is attempting network entry using manual mode for NSP selection and NSPs are available to the IUT as a result of the NSP discovery procedure.
Expected Behaviour	Check that: When the IUT has entered and performed successful authentication to the selected NSP, the IUT indicates the selected NSP.
Test strategy	
Notes	Requires an upper tester.

TP ID	TP/MS/NWE/BV-H0013
Reference	WFNA Stage3 [3]: section 4.1.2.3.2.
PICS Item	
Initial Condition	The IUT is attempting network entry using automatic mode without user intervention and more NSPs are available including the Home NSP.
Expected Behaviour	Check that: The IUT initially selects and attempts authentication with the Home NSP and if successful the IUT indicates the selected NSP.
Test strategy	
Notes	Requires an upper tester.

TP ID	TP/MS/NWE/BV-H002
Reference	WFNA Stage3 [3]: section 4.1.2.2, figure 4-1.
PICS Item	
Initial Condition	The IUT is attempting network discovery.
Expected Behaviour	Check that when the IUT receives a SII-ADV or SBC-RSP with a Base Station ID with the NSP Identifier flag set to ‘0' (indicating only one NSP associated with NAP) no more NSP identification operations are performed.
Test strategy	
Notes	May be difficult to test.

5.2.2 DHCP group

TP ID	TP/MS/DHCP/BV-H000
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: sections 4.8.2.1.2.1 and 4.8.2.1.7.1. RFC 2131 [8]: section 4.3.2.
PICS Item	PIC_DHCPv4.
Initial Condition	MS uses DHCP (and not MIP) for getting its PoA address from the network. The MS has completed initial network entry procedures including authentication and initial service flow (ISF) setup, i.e. initial connection establishment (DSA-REQ/RSP/ACK).
Expected Behaviour	Check that the IUT sends the DHCPDISCOVER message and that the message is formatted per RFC 2131 [8]. Detailed observation results are described in [2] Stage 3: section 4.8.2.1.7.1.
Test strategy	
Notes	

TP ID	TP/MS/DHCP/BV-H001
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: sections 4.8.2.1.2.1 and 4.8.2.1.7.1. RFC 2131 [8]: section 4.3.2.
PICS Item	PIC_DHCPv4
Initial Condition	An ISF exists, and the MS has sent an initial DHCPDISCOVER message to the network over the ISF. The network (TE) has sent a DHCPOFFER message to the MS.
Expected Behaviour	Check that: The MS sends a DHCPREQUEST message to the network over the ISF (Initial Service Flow) and the DHCPREQUEST message is formatted per RFC 2131 [8] (section 4.3.2).
Test strategy	
Notes	

TP ID	TP/MS/DHCP/BV-H002
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: sections 4.8.2.1.2 and 4.8.2.1.7.1. RFC 2131 [8].
PICS Item	PIC_DHCPv4
Initial Condition	The IUT has sent a DHCPREQUEST message to the network, including a previously assigned or previously offered IP address (PoA address), and the TE has confirmed the IP address by sending a DHCPACK message to the IUT.
Expected Behaviour	Check that: When the IUT sends an IP packet, the source address of the IP packet is the assigned IP address.
Test strategy	
Notes	To make the IUT send an IP packet the network may send an IP packet to the IUT requesting a response from the MS, e.g. a "ping" message.

TP ID	TP/MS/DHCP/BV-H003
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: sections 4.8.2.1.2.1 and 4.8.2.1.7.1. RFC 2131 [8]: section 4.3.2.
PICS Item	PIC_DHCPv4.
Initial Condition	An ISF exists, a DHCP renewal has already taken place and the MS has sent a new DHCPDISCOVER message to the network over the ISF. The network (TE) has sent a DHCPOFFER message to the MS.
Expected Behaviour	Check that: The MS sends a DHCPREQUEST message to the network over the ISF (Initial Service Flow) and the DHCPREQUEST message is formatted per RFC 2131 [8] (section 4.3.2).
Test strategy	
Notes	

TP ID	TP/MS/DHCP/BV-H004
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: sections 4.8.2.1.2.1 and 4.8.2.1.7.1. RFC 2131 [8]: section 4.3.2. RFC 2132 [9].
PICS Item	PIC_DHCPv4.
Initial Condition	An ISF exists, and the IUT has sent an initial DHCPDISCOVER message to the network over the ISF. The network (TE) has sent a DHCPOFFER message to the IUT. The IUT has responded by sending a DHCPREQUEST message to select the offered binding.
Expected Behaviour	Check that: When the IUT receives a DHCPACK message with valid parameters, the IUT enters the Bound state.
Test strategy	
Notes	The Bound state can be checked by the discard of e.g. DHCPACK message from TE when in Bound state.

TP ID	TP/MS/DHCP/BV-H005
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: sections 4.8.2.1.2.1 and 4.8.2.1.7.1. RFC 2131 [8]: section 4.3.2. RFC 2132 [9].
PICS Item	PIC_DHCPv4.
Initial Condition	The MS has been assigned a network address (PoA) and a lease time from which timers T1 and T2 are derived. The IUT has sent a DHCPREQUEST message to the address of the DHCP server that allocated the PoA in order to renew the lease time.
Expected Behaviour	Check that: When the IUT receives a DHCPACK message with valid parameters before expiry of timer T2, the IUT returns to state Bound and continues to use the assigned network address.
Test strategy	
Notes	The Bound state can be checked by the discard of e.g. DHCPACK message from TE when in Bound state.

TP ID	TP/MS/DHCP/BV-H006
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: sections 4.8.2.1.2.1 and 4.8.2.1.7.1. RFC 2131 [8]: section 4.3.2. RFC 2132 [9].
PICS Item	PIC_DHCPv4.
Initial Condition	The MS has been assigned a network address (PoA) and a lease time from which timers T1 and T2 are derived. The IUT has sent a DHCPREQUEST message to the address of the DHCP server that allocated the PoA in order to renew the lease time and a second DHCPREQUEST when timer T2 expired in order to rebind the connection.
Expected Behaviour	Check that: When the IUT receives a DHCPACK message with valid parameters before expiry of lease time, the IUT returns to state Bound and continues to use the assigned network address.
Test strategy	
Notes	The Bound state can be checked by the discard of e.g. DHCPACK message from TE when in Bound state.

TP ID	TP/MS/DHCP/BV-H007
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: sections 4.8.2.1.2.1 and 4.8.2.1.7.1. RFC 2131 [8]: section 4.3.2. RFC 2132 [9].
PICS Item	PIC_DHCPv4.
Initial Condition	The MS has been assigned a network address (PoA) and a lease time from which timers T1 and T2 are derived. The IUT has sent a DHCPREQUEST message to the address of the DHCP server that allocated the PoA in order to renew the lease time.
Expected Behaviour	Check that: When the IUT receives a DHCPNAK message before expiry of timer T2, the IUT halts any network connection and sends a new DHCPDISCOVER message.
Test strategy	
Notes	

TP ID	TP/MS/DHCP/BV-H008
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: sections 4.8.2.1.2.1 and 4.8.2.1.7.1. RFC 2131 [8]: section 4.3.2. RFC 2132 [9].
PICS Item	PIC_DHCPv4.
Initial Condition	The MS has been assigned a network address (PoA) and a lease time from which timers T1 and T2 are derived. The IUT has sent a DHCPREQUEST message to the address of the DHCP server that allocated the PoA in order to renew the lease time and a second DHCPREQUEST when timer T2 expired in order to rebind the connection.
Expected Behaviour	Check that: When the IUT received a DHCPNAK message before the lease time has expired, the IUT halts any network connection and sends a new DHCPDISCOVER message.
Test strategy	
Notes	

TP ID	TP/MS/DHCP/BV-H009
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: section 4.8.2.1.1. RFC 2131 [8]: section 3.1.
PICS Item	PIC_DHCPv4.
Initial Condition	An ISF exists, and the IUT has sent an initial DHCPDISCOVER message to the network over the ISF. The network (TE) has sent a DHCPOFFER message to the IUT. The IUT has responded by sending a DHCPREQUEST message to select the offered binding.
Expected Behaviour	Check that: When the IUT receives a DHCPACK message with an address that is already in use, the IUT sends a DHCHDECLINE message and then a new DHCPDISCOVER.
Test strategy	
Notes	

TP ID	TP/MS/DHCP/BV-H010
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: section 4.8.2.1.1. RFC 2131 [8]: section 4.4.6.
PICS Item	PIC_DHCPv4.
Initial Condition	The MS has been assigned a network address (PoA).
Expected Behaviour	Check that: When the IUT no longer needs the assigned network address, the IUT sends DHCPRELEASE message.
Test strategy	
Notes	Requires a means to cause the IUT to e.g. perform a gracefully shut down.

5.2.2.1 DHCP timer

TP ID	TP/MS/DHCP/TI-H000
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: sections 4.8.2.2.7.1, 4.8.2.3.2 and 4.8.2.3.3. RFC 2131 [8]: section 4.4.5. RFC 2132 [9].
PICS Item	PIC_DHCPv4.
Initial Condition	The MS has been assigned a network address (PoA) with and a lease time from which timers T1 and T2 are derived.
Expected Behaviour	Check that: The MS sends a DHCPREQUEST message to the address of the DHCP server that allocated the PoA to the MS no later than at timeout of timer T1.
Test strategy	
Notes	

TP ID	TP/MS/DHCP/TI-H001
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: sections 4.8.2.1.2.1 and 4.8.2.1.7.1. RFC 2131 [8]: section 4.3.2. RFC 2132 [9].
PICS Item	PIC_DHCPv4.
Initial Condition	The MS has been assigned a network address (PoA) and a lease time from which timers T1 and T2 are derived.
Expected Behaviour	Check that: The IUT sends a DHCPREQUEST message to the address of the DHCP server that allocated the PoA to the IUT no later than at timeout of timer T1 and if no DHCPACK or DHCPNAK is received before expiry of timer T2 the IUT sends a DHCPREQUEST message to the IP broadcast address "0xffffffff".
Test strategy	
Notes	

TP ID	TP/MS/DHCP/TI-H002
Reference	WFNA Stage2p2 [2]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [3]: sections 4.8.2.1.2.1 and 4.8.2.1.7.1. RFC 2131 [8]: section 4.3.2. RFC 2132 [9].
PICS Item	PIC_DHCPv4.
Initial Condition	The MS has been assigned a network address (PoA) and a lease time from which timers T1 and T2 are derived. The timers T1 and T2 has expired and the IUT has sent a DHCPREQUEST message for renewing the lease time followed by a DHCPREQUEST to rebind to the DHCP server.
Expected Behaviour	Check that: When the lease time expires and no DHCPACK or DHCPNAK messages have been received, the IUT halts any network connection and sends a new DHCPDISCOVER message.
Test strategy	
Notes	

5.2.3 CMIPv4

TP ID	TP/MS/CMIPV4/BV-H000
Reference	WFNA Stage2p2 [2]: section 7.8.1.9.1. WFNA Stage3 [3]: section 4.8.3.1. RFC 3344 [10].
PICS Item	PIC_CMIPV4.
Initial Condition	The MS has completed the authentication process shown in Stage-2 figure 7-70 step 1. Binding of MS flow to intra-ASN data path as shown in stage-2 figure 7-70 step 2 is complete. The MS will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage-3 section 4.3.5]. The MS has the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage-3 section 4.3.1]. The MS has the out NAI (bootstrapped during normal authentication phase) [See Stage-3 section 4.4.1.3.1]. The Network has sent a Mobile IP Agent Advertisement message to the MS that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10], section 2.1.
Expected Behaviour	Check that: the MS shall generate and send a MIPv4 registration request message to the foreign agent with the HA field set to 255.255.255.255 or 0.0.0.0 when requesting dynamic HA assignment.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H001
Reference	WFNA Stage2p2 [2]: section 7.8.1.9.1. WFNA Stage3 [3]: section 4.8.3.1. RFC 3344 [10].
PICS Item	PIC_CMIPV4.
Initial Condition	The MS has completed the authentication process shown in Stage-2 figure 7-70 step 1. Binding of MS flow to intra-ASN data path as shown in stage-2 figure 7-70 step 2 is complete. The MS will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage-3 section 4.3.5]. The MS has the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage-3 section 4.3.1]. The MS has the out NAI (bootstrapped during normal authentication phase) [See Stage-3 section 4.4.1.3.1]. The Network has sent a Mobile IP Agent Advertisement message to the MS that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10], section 2.1.
Expected Behaviour	Check that: the IUT generates and send a MIPv4 registration request message to the foreign agent with the HA field set to the HA address when the IUT knows the HA address.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H002
Reference	WFNA Stage2p2 [2]: section 7.8.1.9.2. WFNA Stage3 [3]: section 4.8.3.2. RFC 3344 [10].
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has completed authentication and mobile IP registration (and received a value for the lifetime timer during registration), and the TE has provided a properly formatted MIP re-Registration Reply based on the IUT Registration Request. The IUT has the MN-HA Key (bootstrapped during normal authentication phase) [See Stage-3 section 4.3.5], the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage-3 section 4.3.1], and the out NAI (bootstrapped during normal authentication phase) [See Stage-3 section 4.4.1.3.1].
Expected Behaviour	When the current lifetime timer is approaching 0, or any predefined value the IUT shall send a MIPv4 re-registration request message requesting an update to the registration lifetime timer. The request shall be formatted per per RFC 3344 [10], section 3.3 and any necessary extensions shall be included. The NAI Extension with the pseudo NAI (pseudoIdentity@realm) SHALL be included in the re- registration message. MN-HA SHALL be included in the re-registration message. MN-FA MAY be included in the re-registration message.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H003
Reference	WFNA Stage2p2 [2]: section 7.8.1.9.5. WFNA Stage3 [3]: section 4.8.3.4. RFC 3344 [10].
PICS Item	PIC_CMIPV4.
Initial Condition	The IUT has completed authentication and mobile IP registration. The TE has sent a formatted MIP Registration Reply based on the MS Registration Request. The IUT has the MN-HA Key (bootstrapped during normal authentication phase) [See Stage-3 section 4.3.5], the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage-3 section 4.3.1], and the out NAI (bootstrapped during normal authentication phase) [See Stage-3 section 4.4.1.3.1].
Expected Behaviour	Check that to the MS sends a registration message with a lifetime timer=0 to initiate session termination. The network replies with a registration reply indicating the lifetime timer=0. Verify that the registration message is formatted per RFC 3344 [10], section 3.3 and any necessary extensions are included. The NAI Extension with the pseudo NAI (pseudoIdentity@realm) SHALL be included in the registration message. MN-HA SHALL be included in the registration message. MN-FA MAY be included in the registration message.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H004
Reference	WFNA Stage2p2 [2]: section 7.8.1.9.3. WFNA Stage3 [3]: section 4.8.3.3. RFC 3344 [10].
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has a CMIPv4 session active with a session established with MN-HA key, CMIPv4 SPI, and NAI.
Expected Behaviour	Check that: Upon receipt of the CMIPv4 agent advertisement the MS sends a mobile IPv4 registration request message to the CoA identified in the agent advertisement message. Verify the registration message is formatted per RFC 3344 [10], section 3.3 and any necessary extensions are included. The NAI Extension with the pseudo NAI (pseudoIdentity@realm) SHALL be included on the registration message. MN-HA SHALL be included in the registration message. MN-FA MAY be included in the registration message.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H005
Reference	WFNA Stage2p2 [2]: section 7.8.1.9.3. WFNA Stage3 [3]: section 4.8.3.3. RFC 3344 [10]: sections 2.2 and 2.4. RFC 1256 [6]: sections 3 and 5.1.
PICS Item	PIC_CMIPV4.
Initial Condition	The MS has completed the authentication process shown in Stage-2 figure 7-70 step 1. Binding of MS flow to intra-ASN data path as shown in stage-2 figure 7-70 step 2 is complete. The MS will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage-3 section 4.3.5]. The MS has the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage-3 section 4.3.1]. The MS has the outer NAI (bootstrapped during normal authentication phase) [See Stage-3 section 4.4.1.3.1]. No Agent Advertisement message has been sent and no care-of-address has been determined.
Expected Behaviour	Check that: The IUT sends an Agent Solicitation message with the TTL field set to 1 in order to request an Agent Advertisement message to be sent.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H006
Reference	WFNA Stage2p2 [2]: section 7.8.1.9.3. WFNA Stage3 [3]: section 4.8.3.3. RFC 3344 [10]: sections 2.2 and 2.4. RFC 1256 [6]: sections 3 and 5.1.
PICS Item	PIC_CMIPV4
Initial Condition	The MS has completed the authentication process shown in Stage-2 figure 7-70 step 1. Binding of MS flow to intra-ASN data path as shown in stage-2 figure 7-70 step 2 is complete. The MS will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage-3 section 4.3.5]. The MS has the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage-3 section 4.3.1]. The MS has the outer NAI (bootstrapped during normal authentication phase) [See Stage-3 section 4.4.1.3.1]. No Agent Advertisement message has been sent and no care-of-address has been determined.
Expected Behaviour	Check that: The IUT as a first attempt sends a maximum of 3 Agent Solicitation messages with a maximum rate of one per second.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H007
Reference	WFNA Stage2p2 [2]: section 7.8.1.9.3. WFNA Stage3 [3]: section 4.8.3.3. RFC 3344 [10]: sections 2.2 and 2.4. RFC 1256 [6]: sections 3 and 5.1.
PICS Item	PIC_CMIPV4.
Initial Condition	The MS has completed the authentication process shown in Stage-2 figure 7-70 step 1. Binding of MS flow to intra-ASN data path as shown in stage-2 figure 7-70 step 2 is complete. The MS will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage-3 section 4.3.5]. The MS has the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage-3 section 4.3.1]. The MS has the outer NAI (bootstrapped during normal authentication phase) [See Stage-3 section 4.4.1.3.1]. No Agent Advertisement message has been sent and no care-of-address has been determined.
Expected Behaviour	Check that: When the IUT sends Agent Solicitation messages for which it does not receive any Agent Advertisement message the IUT uses exponential backoff mechanism doubling the interval until the next transmission of consecutive Agent Solicitation messages.
Test strategy	
Notes	

5.2.4 QoS

TP ID	TP/MS/QoS/BV-H000
Reference	WFNA Stage2p2 [2]: section 7.6. IEEE 802.16e [5]: sections 6.3.14.7.1.2 and 6.3.14.9.3.2.
PICS Item	
Initial Condition	IUT is operational. The TE has sent a DSA-REQ to the IUT to request creation of a UL service flow with QoS parameters supported by QoS capabilities of the IUT.
Expected Behaviour	Check that: the IUT sends a DSA-RSP message indicating acceptance.
Test strategy	
Notes	

TP ID	TP/MS/QoS/BV-H001
Reference	WFNA Stage2p2 [2]: section 7.6. IEEE 802.16e [5]: sections 6.3.14.7.1.2 and 6.3.14.9.3.2.
PICS Item	
Initial Condition	IUT is operational. The TE has sent a DSA-REQ to the IUT to request creation of a UL service flow for which the QoS parameters are not supported by QoS capabilities of the IUT.
Expected Behaviour	Check that: the IUT sends a DSA-RSP message indicating rejection.
Test strategy	
Notes	

TP ID	TP/MS/QoS/BV-H002
Reference	WFNA Stage2p2 [2]: section 7.6. IEEE 802.16e [5]: sections 6.3.14.7.1.2 and 6.3.14.9.3.2.
PICS Item	
Initial Condition	IUT is operational. The TE has sent a DSA-REQ to the IUT to request creation of a DL service flow with QoS parameters supported by QoS capabilities of the IUT.
Expected Behaviour	Check that: the IUT sends a DSA-RSP message indicating acceptance.
Test strategy	
Notes	

TP ID	TP/MS/QoS/BV-H003
Reference	WFNA Stage2p2 [2]: section 7.6. IEEE 802.16e [5]: section 6.3.14.7.1.2 and 6.3.14.9.3.2.
PICS Item	
Initial Condition	IUT is operational. The TE has sent a DSA-REQ to the IUT to request creation of a DL service flow with QoS parameters that are not supported by the QoS capabilities of the IUT.
Expected Behaviour	Check that: the IUT sends a DSA-RSP message indicating rejection.
Test strategy	
Notes	

5.2.5 Security

TP ID	TP/MS/SEC/BV-H000
Reference	WFNA Stage3 [3]: section 4.4.1.4.1.1. RFC 3748 [13]: section 4.2.
PICS Item	
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed.
Expected Behaviour	Check that: When the IUT receives an EAP-Failure message and the EAP method is reset the IUT attempts to re-enter the network.
Test strategy	
Notes	Requires a means to ensure that the IUT attempts to re-enter after EAP failure.

TP ID	TP/MS/SEC/BV-H001
Reference	WFNA Stage3 [3]: section 4.4.1.4.1.1.
PICS Item	
Initial Condition	The IUT is performing initialization and is entering Authorization phase.
Expected Behaviour	Check that: when the IUT receives an EAP-Request Identity message, the IUT responds with an EAP-Response Identity message containing the NAI with a realm part which is the Fully Qualified Domain Name (FQDN) of the Home Connectivity Service Network.
Test strategy	
Notes	

5.2.5.1 Device authentication

TP ID	TP/MS/SEC/EAPTLS/BV-H000
Reference	RFC 5216 [7]: section 3.1. WFNA Stage3 [3]: section 4.4.1.2.1.
PICS Item	
Initial Condition	1) The TE has its own certificate to be used for the server certificate. 2) The MS also has its certificate and CA certificate. 3) Capability negotiation (SBC-REQ/RSP) has been successfully completed.
Expected Behaviour	Check that: When the IUT receives an EAP-Request/Identity, the IUT responds with an EAP-Response/Identity with NAI. Verify that the username part of NAI is the MAC Address of the IUT that is six pairs of hexadecimal digits expressed as uppercase letters.
Test strategy	
Notes	The MAC address is six pairs of hexadecimal digits, e.g. "006021A50A23" (see section 4.4.1.2.1 of [3]).

TP ID	TP/MS/SEC/EAPTLS/BV-H001
Reference	RFC 5216 [7]: section 3.1. WFNA Stage3 [3]: section 4.4.1.2.1.
PICS Item	
Initial Condition	1) The TE has its own certificate to be used for the server certificate. 2) The MS also has its certificate and Certification Authorization (CA) certificate. 3) Capability negotiation (SBC-REQ/RSP) has been successfully completed and device authentication has started. The IUT has received an EAP-Request/Identity and responded with a valid EAP-Response/Identity message.
Expected Behaviour	Check that: When the IUT receives EAP-Request/EAP-Type=EAP-TLS with TLS Start, the IUT responds with an EAP-Response/EAP-Type with TLS client_hello.
Test strategy	
Notes	

TP ID	TP/MS/SEC/EAPTLS/BV-H002
Reference	RFC 5216 [7]: section 3.1. WFNA Stage3 [3]: section 4.4.1.2.1.
PICS Item	
Initial Condition	1) The TE has its own certificate to be used for the server certificate. 2) The MS also has its certificate and Certification Authorization (CA) certificate. 3) Capability negotiation (SBC-REQ/RSP) has been successfully completed and device authentication is in progress. The IUT has sent a valid EAP-Response/EAP-Type=EAP-TLS message with parameter TLS client_hello in response to an EAP-Request message with parameter TLS Start.
Expected Behaviour	Check that: When the TE sends EAP-Request/EAP-Type=EAP-TLS with TLS server_hello, TLS certificate, TLS certificate_request, TLS server_hello_done with Null CipherSuite and null compression_method in server_hello, the IUT responds with an EAP-Response/EAP-Type=EAP-TLS with TLS certificate, TLS client_key_exchange, TLS certificate_verify, TLS change_cipher_spec and TLS finished.
Test strategy	
Notes	Note that the EAP-TLS message MUST be fragmented if the message size is greater than MTU size (1400B). See the section 4.4.1.2.1 of NWG Stage 3.

TP ID	TP/MS/SEC/EAPTLS/BV-H003
Reference	RFC 5216 [7]. WFNA Stage3 [3]: section 4.4.1.2.1.
PICS Item	
Initial Condition	1) The TE has its own certificate to be used for the server certificate. 2) The MS also has its certificate and Certification Authorization (CA) certificate. 3) Capability negotiation (SBC-REQ/RSP) has been successfully completed and device authentication for a new session is in progress. The IUT has sent an EAP-Response/EAP-Type=EAP TLS with "TLS client_key_exchange", "TLS change_cipher_spec", and "TLS finished" parameters in response to an EAP-Request/EAP-Type=EAP TLS with "service_certificate" and "server_hello_done" handshake parameters.
Expected Behaviour	Check that: When the TE sends EAP-Request/EAP-Type=EAP-TLS with "TLS change_cipher_spec" and "TLS finished" parameters , the IUT responds by sending an EAP-Response/EAP-Type=EAP-TLS and with no data.
Test strategy	
Notes	

5.2.5.1.1 Retry behaviour

TP ID	TP/MS/SEC/EAPTLS/BV-H004
Reference	RFC 5216 [7]: section 3.2. WFNA Stage3 [3]: section 4.4.1.2.1.
PICS Item	
Initial Condition	1) The TE has its own certificate to be used for the server certificate. 2) The MS also has its certificate and Certification Authorization (CA) certificate. 3) Capability negotiation (SBC-REQ/RSP) has been successfully completed. The IUT has started EAP authorization and has responded to the EAP-Request/Identity.
Expected Behaviour	Check that: When the IUT receives the EAP-Request with TLS Start parameter, the IUT sends an EAP-Response with a TLS client_hello parameter, and that if after this another EAP-Request message with TLS Start parameter is received the IUT again sends the EAP-Response message with TLS client_hello parameter.
Test strategy	
Notes	

5.2.5.1.2 Fragmentation

TP ID	TP/MS/SEC/EAPTLS/FRAG/BV-H000
Reference	RFC 5216 [7]: section 3.3. WFNA Stage3 [3]: section 4.4.1.2.1.
PICS Item	
Initial Condition	1) The TE has its own certificate to be used for the server certificate. 2) The MS also has its certificate and Certification Authorization (CA) certificate. 3) Capability negotiation (SBC-REQ/RSP) has been successfully completed. The IUT is receiving fragmented TLS messages.
Expected Behaviour	Check that: When the IUT receives a fragment of a TLS message in an EAP-Request, the IUT acknowledges the reception by sending an EAP-Response with EAP-Type=EAP-TLS, no data, and with the same Identifier value as received in the EAP-Request.
Test strategy	
Notes	

TP ID	TP/MS/SEC/EAPTLS/ FRAG/BV-H001
Reference	RFC 5216 [7]: section 3.3. WFNA Stage3 [3]: section 4.4.1.2.1.
PICS Item	
Initial Condition	1) The TE has its own certificate to be used for the server certificate. 2) The MS also has its certificate and Certification Authorization (CA) certificate. 3) Capability negotiation (SBC-REQ/RSP) has been successfully completed. The IUT is transmitting a fragmented TLS message in EAP-Response packets.
Expected Behaviour	Check that: Only when the IUT receives an acknowledgement EAP-Request message from the TE, it sends the next fragment message in an EAP-Response message using the incremented Identifier value of the received acknowledgement EAP-Request.
Test strategy	
Notes	

TP ID	TP/MS/SEC/EAPTLS/ FRAG/BV-H002
Reference	WFNA Stage3 [3]: section 4.4.1.2.1.
PICS Item	
Initial Condition	The IUT has successfully completed capability negotiation (SBC-REQ/RSP). The IUT is performing device authentication using the EAP-TLS procedure.
Expected Behaviour	Check that: The IUT use EAP-TLS fragmentation to transmit TLS messages when the MTU size exceeds 1 400 Bytes.
Test strategy	
Notes	

5.2.5.2 User authentication

5.2.5.2.1 EAP-AKA

TP ID	TP/MS/SEC/EAPAKA/BV-H000
Reference	RFC 4187 [11]. WFNA Stage3 [3]: section 4.4.1.2.1. ETSI/3GPP Auth and Key Generation Functions (TS 155 205 [25]).
PICS Item	PIC_EAPAKA
Initial Condition	The IUT and TE are configured to have the same value of K and OPc for credentials defined in TS 155 205 [25] in order to generate the valid authentication vectors. Capability negotiation (SBC-REQ/RSP) has been successfully completed.
Expected Behaviour	Check that: When the TE sends an EAP-Request/Identity, the IUT responds with EAP-Response/Identity with NAI.
Test strategy	
Notes	

TP ID	TP/MS/SEC/EAPAKA/BV-H001
Reference	RFC 4187 [11]. WFNA Stage3 [3]: section 4.4.1.2.1. ETSI/3GPP Auth and Key Generation Functions (TS 155 205 [25]).
PICS Item	PIC_EAPAKA
Initial Condition	The IUT and TE are configured to have the same value of K and OPc for credentials defined in TS 155 205 [25] in order to generate the valid authentication vectors. Capability negotiation (SBC-REQ/RSP) has been successfully completed and EAP-AKA user authentication started. The IUT has sent an EAP-Response/Identity in response to an EAP-Request/Identity message from the TE.
Expected Behaviour	Check that: When the TE sends EAP-Request/AKA-Challenge with AT_RAND, AT_AUTN, AT_MAC, the IUT responds with a valid EAP-Response/AKA-Challenge with AT_RES, AT_MAC parameters.
Test strategy	
Notes	

5.2.5.2.1.1 Responses in case of non-valid parameters

TP ID	TP/MS/SEC/EAPAKA/BV-H002
Reference	RFC 4187 [11]: sections 6.3.1 and 9.5. WFNA Stage3 [3]: section 4.4.1.2.1. ETSI/3GPP Auth and Key Generation Functions (TS 155 205 [25]).
PICS Item	PIC_EAPAKA
Initial Condition	The IUT and TE are configured to have the same value of K and OPc for credentials defined in TS 155 205 [25] in order to generate the valid authentication vectors. Capability negotiation (SBC-REQ/RSP) has been successfully completed and EAP-AKA user authentication started. The IUT has sent an EAP-Response/Identity in response to an EAP-Request/Identity message from the TE.
Expected Behaviour	Check that: When the TE sends EAP-Request/AKA-Challenge with AT_RAND, AT_AUTN, AT_MAC where the AUTN value is incorrect, the IUT responds with an EAP-Response/AKA-Authentication-Reject message due to failing verification of the AUTN value.
Test strategy	
Notes	

TP ID	TP/MS/SEC/EAPAKA/BV-H003
Reference	RFC 4187 [11]: sections 6.3.1 and 9.5. WFNA Stage3 [3]: section 4.4.1.2.1. ETSI/3GPP Auth and Key Generation Functions (TS 155 205 [25]).
PICS Item	PIC_EAPAKA
Initial Condition	The IUT and TE are configured to have the same value of K and OPc for credentials defined in TS 155 205 [25] in order to generate the valid authentication vectors. Capability negotiation (SBC-REQ/RSP) has been successfully completed and EAP-AKA user authentication started. The IUT has sent an EAP-Response/Identity in response to an EAP-Request/Identity message from the TE.
Expected Behaviour	Check that: When the TE sends EAP-Request/AKA-Challenge with AT_RAND, AT_AUTN, AT_MAC where AUTN has an inappropriate sequence number, the IUT responds with an EAP-Response/AKA-Synchronization-Failure message with parameter AT_AUTS.
Test strategy	
Notes	

TP ID	TP/MS/SEC/EAPAKA/BV-H004
Reference	RFC 4187 [11]: section 6.3.1. WFNA Stage3 [3]: section 4.4.1.2.1. ETSI/3GPP Auth and Key Generation Functions (TS 155 205 [25]).
PICS Item	PIC_EAPAKA
Initial Condition	The IUT and TE are configured to have the same value of K and OPc for credentials defined in TS 155 205 [25] in order to generate the valid authentication vectors. Capability negotiation (SBC-REQ/RSP) has been successfully completed and EAP-AKA user authentication started. The IUT has sent an EAP-Response/Identity in response to an EAP-Request/Identity message from the TE.
Expected Behaviour	Check that: When the TE sends EAP-Request/AKA-Challenge with a malformed attribute, the IUT responds with an EAP-Response/AKA-Client-Error message with error code 0 "unable to process packet".
Test strategy	
Notes	

TP ID	TP/MS/SEC/EAPAKA/BV-H005
Reference	RFC 4187 [11]: section 6.1. WFNA Stage3 [3]: section 4.4.1.2.2. ETSI/3GPP Auth and Key Generation Functions (TS 155 205 [25]).
PICS Item	PIC_EAPAKA
Initial Condition	The IUT and TE are configured to have the same value of K and OPc for credentials defined in TS 155 205 [25] in order to generate the valid authentication vectors. Capability negotiation (SBC-REQ/RSP) has been successfully completed and EAP-AKA user authentication started. The IUT has sent an EAP-Response/Identity in response to an EAP-Request/Identity message from the TE and the IUT has responded to an EAP-Request/AKA-Challenge with an EAP-Response/AKA-Challenge.
Expected Behaviour	Check: That when the IUT receives a EAP-Request/AKA-Notification with the S-bit set to zero (indicating failure) and the P-bit set to 1 (indicating that the EAP-AKA challenge procedure was not completed), the IUT responds with a EAP-Response/AKA-Notification.
Test strategy	
Notes	

5.2.5.2.2 EAP-TTLS

TP ID	TP/MS/SEC/EAPTTLSv0/BV-H000
Reference	draft-ietf-pppext -eap-ttls-05 [12]. WFNA Stage3 [3]: section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed and user authentication based on EAP-TTLS started.
Expected Behaviour	Check that: When the IUT receives an EAP-Request/Identity message, the IUT responds with an EAP-Response/Identity message with NAI.
Test strategy	
Notes	The TE has its own certificate to be used for the server certificate and the TE uses this to verify the MS certificate, by sending Certificate Request.

TP ID	TP/MS/SEC/EAPTTLSv0/BV-H001
Reference	draft-ietf-pppext -eap-ttls-05 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [3]: section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed and user authentication based on EAP-TTLS started. The IUT has sent an EAP-Response/Identity message with NAI in response to an EAP-Request/Identity message from the TE.
Expected Behaviour	Check that: When the IUT receives an EAP-Request/EAP-Type=EAP-TTLS with Start Bit set to 1, the IUT responds with an EAP-Response/EAP-Type=EAP-TTLS with ClientHello.
Test strategy	
Notes	The TE has its own certificate to be used for the server certificate and the TE uses this to verify the MS certificate, by sending Certificate Request.

TP ID	TP/MS/SEC/EAPTTLSv0/BV-H002
Reference	draft-ietf-pppext -eap-ttls-05 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [3]: section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed and user authentication based on EAP-TTLS started. The IUT has responded to an EAP-Request/Identity and sent an EAP-Response with ClientHello parameter in response to an EAP-Request with parameter TTLS-Start.
Expected Behaviour	Check that: When the IUT receives an EAP-Request/EAP-Type=EAP-TLS message with ServerHello, Certificate, CertificateRequest, and ServerHelloDone, the IUT responds EAP-Response/EAP-Type=EAP-TTLS with Certificate, ClientKeyExchange, CertificateVerify, ChangeCipherSpec and Finished.
Test strategy	
Notes	The TE has its own certificate to be used for the server certificate and the TE uses this to verify the MS certificate, by sending Certificate Request. Note that the EAP-TLS message MUST be fragmented if the message size is greater than MTU size (1400B). See the section 4.4.1.2.3 of NWG Stage 3.

TP ID	TP/MS/SEC/EAPTTLSv0/BV-H003
Reference	draft-ietf-pppext -eap-ttls-05 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [3]: section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed and user authentication based on EAP-TTLS started. The IUT has provided the NAI to the TE and completed the TLS 3-way handshake by the IUT sending an EAP-Response with the "Finished" parameter and then received an EAP-Request with "Finished" parameter.
Expected Behaviour	Check that: The IUT responds to the EAP-Request with Finished parameter by sending an EAP-Response/EAP-Type=EAP-TTLS with User-Name, MS-CHAP-Challenge, and MS-CHAP2-Response AVP to enable the TE to perform user authentication.
Test strategy	
Notes	The TE has its own certificate to be used for the server certificate and the TE uses this to verify the MS certificate, by sending Certificate Request.

TP ID	TP/MS/SEC/EAPTTLSv0/BV-H004
Reference	draft-ietf-pppext -eap-ttls-05 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [3]: NWG Stage 3 section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed and user authentication based on EAP-TTLS started. The IUT has provided the NAI to the TE and successfully completed TLS 3-way handshake and started user Authentication by sending an EAP-Response with parameters User-Name, MS-CHAP-Challenge and MS-CHAP2-Response AVPs.
Expected Behaviour	Check that: When IUT receives an EAP-Request/EAP-Type=EAP-TTLS with MS-CHAP2-Success AVP parameter, the IUT responds EAP-Response/EAP-Type= EAP-TTLS with no data.
Test strategy	
Notes	The TE has its own certificate to be used for the server certificate and the TE uses this to verify the MS certificate, by sending Certificate Request.

TP ID	TP/MS/SEC/EAPTTLSv0/BV-H005
Reference	draft-ietf-pppext -eap-ttls-05 [12]. WFNA Stage3 [3]: section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed and user authentication based on EAP-TTLS started.
Expected Behaviour	Check that: When IUT receives an EAP-Request/Identity, the IUT responds with an EAP-Response/Identity with NAI.
Test strategy	
Notes	The TE has its own certificate to be used for the server certificate but the TE does not send CertificateRequest.

TP ID	TP/MS/SEC/EAPTTLSv0/BV-H006
Reference	draft-ietf-pppext -eap-ttls-05 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [3]: section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed and user authentication based on EAP-TTLS started. The IUT has sent an EAP-Response/Identity message with NAI in response to an EAP-Request/Identity message from the TE.
Expected Behaviour	Check that: When the IUT receives an EAP-Request/EAP-Type=EAP-TTLS with Start Bit set to 1, the IUT responds with an EAP-Response/EAP-Type=EAP-TTLS with ClientHello.
Test strategy	
Notes	The TE has its own certificate to be used for the server certificate but the TE does not send CertificateRequest.

TP ID	TP/MS/SEC/EAPTTLSv0/BV-H007
Reference	draft-ietf-pppext -eap-ttls-05 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [3]: section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed and user authentication based on EAP-TTLS started. The IUT has responded to an EAP-Request/Identity and sent an EAP-Response with ClientHello parameter in response to an EAP-Request with parameter TTLS-Start.
Expected Behaviour	Check that: When IUT receives an EAP-Request/EAP-Type=EAP-TLS with ServerHello, Certificate, and ServerHelloDone, the IUT responds with an EAP-Response/EAP-Type=EAP-TTLS with ClientKeyExchange, ChangeCipherSpec and Finished parameters.
Test strategy	
Notes	The TE has its own certificate to be used for the server certificate but the TE does not send CertificateRequest. Note that the EAP-TLS message MUST be fragmented if the message size is greater than MTU size (1 400 B). See the section 4.4.1.2.3 of NWG Stage 3.

TP ID	TP/MS/SEC/EAPTTLSv0/BV-H008
Reference	draft-ietf-pppext -eap-ttls-05 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [3]: section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed and user authentication based on EAP-TTLS started. The IUT has provided the NAI to the TE and completed the TLS 3-way handshake by the IUT sending an EAP-Response with the "Finished" parameter and then received an EAP-Request with "Finished" parameter.
Expected Behaviour	Check that: The IUT in response to the EAP-Request message with Finished parameters sends an EAP-Response/EAP-Type=EAP-TTLS with User-Name, MS-CHAP-Challenge, and MS-CHAP2-Response AVP to enable the TE to perform user authentication.
Test strategy	
Notes	The TE has its own certificate to be used for the server certificate but the TE does not send CertificateRequest.

TP ID	TP/MS/SEC/EAPTTLSv0/BV-H009
Reference	draft-ietf-pppext -eap-ttls-05 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [3]: section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed and user authentication based on EAP-TTLS started. The IUT has provided the NAI to the TE and successfully completed TLS 3-way handshake and started user Authentication by sending an EAP-Response with parameters User-Name, MS-CHAP-Challenge and MS-CHAP2-Response AVPs.
Expected Behaviour	Check that: When the IUT receives an EAP-Request/EAP-Type=EAP-TTLS with MS-CHAP2-Success AVP, the IUT responds with EAP-Response/EAP-Type= EAP-TTLS with no data.
Test strategy	
Notes	The TE has its own certificate to be used for the server certificate but the TE does not send CertificateRequest.

5.2.5.2.2.1 EAP-TTLS Fragmentation

TP ID	TP/MS/SEC/EAPTTLSv0/FRAG/BV-H000
Reference	draft-ietf-pppext -eap-ttls-05 [12]: section 8.2. WFNA Stage3 [3]: section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed, the authentication procedure has started and the IUT is receiving a fragmented TTLS message.
Expected Behaviour	Check that: When the IUT receives a fragment of a TTLS message in an EAP-Request, the IUT acknowledges the reception by sending an EAP-Response with EAP-Type=EAP-TTLS, no data, and with the same Identifier value as received in the EAP-Request.
Test strategy	
Notes	

TP ID	TP/MS/SEC/EAPTTLSv0/FRAG/BV-H001
Reference	draft-ietf-pppext -eap-ttls-05 [12]: section 8.2. WFNA Stage3 [3]: section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	Capability negotiation (SBC-REQ/RSP) has been successfully completed, the authentication procedure has started and the IUT is transmitting a fragmented TTLS message.
Expected Behaviour	Check that: Only when the IUT receives an acknowledgement EAP-Request/ EAP-Type=TTLS message from the TE, it sends the next fragment message in an EAP-Response/EAP-Type=TTLS message using the incremented Identifier value of the received acknowledgement EAP-Request.
Test strategy	

TP ID	TP/MS/SEC/EAPTTLSv0/FRAG/BV-H002
Reference	WFNA Stage3 [3]: section 4.4.1.2.3.
PICS Item	PIC_EAPTTLS.
Initial Condition	The IUT has successfully completed capability negotiation (SBC-REQ/RSP). The IUT is performing user authentication using the EAP-TTLS procedure.
Expected Behaviour	Check that: The IUT use EAP-TLS fragmentation to transmit TTLS messages when the MTU size exceeds 1 400 Bytes.
Test strategy	

5.2.5.3 CMAC Keys

TP ID	TP/MS/SEC/CMAC/BV-H000
Reference	WFNA Stage3 [3]: section 4.3.4.1.
PICS Item	
Initial Condition	The IUT has successfully completed PKMv2 authentication.
Expected Behaviour	Check that: In subsequent initial RNG-REQ messages the included TLV CMAC_KEY_COUNT value is incremented by one for each RNG-REQ message sent by the IUT.
Test strategy	
Notes	

TP ID	TP/MS/SEC/CMAC/BV-H001
Reference	WFNA Stage3 [3]: section 4.3.4.1.1.
PICS Item	
Initial Condition	The IUT is performing network handover to a new target BS.
Expected Behaviour	Check that: The IUT sends RNG-REQ messages to potential target BSs using the same CMAC_KEY_COUNT value in all requests.
Test strategy	
Notes	

5.2.6 IPv6

TP ID	TP/MS/IPv6 /BV-H000
Reference	WFNA Stage2p2 [2]: section 7.2.2. WFNA Stage3 [3]: section 4.11.4. RFC 4861 [14]. RFC 3315 [16]: section 5.3.
PICS Item	
Initial Condition	The IUT has successfully completed network entry and device authentication. During authentication DHCPv6 server information is included.
Expected Behaviour	Check that: the IUT sends a DHCPv6 REQUEST message (msg type 3) requesting an IPv6 address to the DHCPv6 server identified during authentication.
Test strategy	
Notes	

TP ID	TP/MS/IPv6 /BV-H001
Reference	WFNA Stage2p2 [2]: section 7.2.2. WFNA Stage3 [3]: section 4.11.4. RFC 4861 [14]. RFC 4862 [15].
PICS Item	
Initial Condition	IUT has completed authentication.
Expected Behaviour	Check that: When the IUT receives a Router Advertisement message, the MS performs stateless autoconfiguration of its IP address as defined in RFC 4862 [15] and performs duplicate address detection (DAD) by sending a Neighbor Solicitation message.
Test strategy	
Notes	

TP ID	TP/MS/IPv6 /BV-H002
Reference	WFNA Stage2p2 [2]: section 7.2.2. WFNA Stage3 [3]: section 4.11.4. RFC 4861 [14]. RFC 4862 [15].
PICS Item	
Initial Condition	IUT has completed authentication and the IUT is IPv6 capable.
Expected Behaviour	Check that: MS shall sends a IPv6 Router Solicitation message to start stateless IP configuration.
Test strategy	
Notes	In response to the Router Solicitation message the network should generate and send a Router Advertisement message. The MS would then follow normal stateless autoconfig procedures defined in RFC 4861 [14] (but this is a different TP).

TP ID	TP/MS/IPv6 /BV-H003
Reference	WFNA Stage3 [3]: section 4.11.3. RFC 4861 [14]. RFC 4862 [15].
PICS Item	
Initial Condition	IUT has completed of IPv6 Initial Service Flow and has sent a Router Solicitation message.
Expected Behaviour	Check that: if the IUT does not receive Router Advertisement message in response to the Router Solicitation message, the IUT initiates network exit and re-entry procedures.
Test strategy	
Notes	Requires a means to make the IUT send a Router Solicitation message.

TP ID	TP/MS/IPv6 /BV-H004
Reference	WFNA Stage3 [3]: section 4.11.3. RFC 4861 [14]. RFC 4862 [15].
PICS Item	
Initial Condition	IUT has completed of IPv6 Initial Service Flow.
Expected Behaviour	Check that: if the IUT does not receive Router Advertisement message, the IUT initiates network exit and re-entry procedures.
Test strategy	
Notes	

5.2.7 CMIPv6

TP ID	TP/MS/CMIPv6/BV-H000
Reference	WFNA Stage2p2 [2]: section 7.8.2.5.1. WFNA Stage3 [3]: section 4.8.4.1. RFC 3775 [17]: section 6.1.7. RFC 4285 [18].
PICS Item	PIC_CMIPv6.
Initial Condition	IUT has completed IPv6 Address assignment using either stateful or stateless IP configuration.
Expected Behaviour	Check that: The IUT sends a Binding Update message with the Destination Option Header and mobility header (MH type 5). It may include the MN-NA, mobility option, MSG-option ID, and MN-HA authentication option.
Test strategy	
Notes	

TP ID	TP/MS/CMIPv6/BV-H001
Reference	WFNA Stage2p2 [2]: section 7.8.2.5.3. WFNA Stage3 [3]: section 4.8.4.2. RFC 3775 [17].
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is currently involved in a CMIPv6 session.
Expected Behaviour	Check that: when the IUT receives a new Router Advertisement containing a new prefix, the IUT sends a new binding update (BU) message with a new IP address based on the prefix received in the router advertisement.
Test strategy	
Notes	If stateless IP address configuration is used to calculate the new CoA then DAD shall also be preformed.

TP ID	TP/MS/CMIPv6/BV-H002
Reference	WFNA Stage2p2 [2]: section 7.8.2.5.2. WFNA Stage3 [3]: section 4.8.4.3. RFC 3775 [17].
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is currently involved in a CMIPv6 session.
Expected Behaviour	Check that: when the lifetime timer received in the initial binding update message expires, the IUT sends a new biding update message using the same credentials that were assigned in the previous binding update, with the exception the IUT will requests a new lifetime timer value.
Test strategy	
Notes	

TP ID	TP/MS/CMIPv6/BV-H003
Reference	WFNA Stage2p2 [2]: section 7.8.2.5.5. WFNA Stage3 [3]: section 4.8.4.4. RFC 3775 [17].
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is currently involved in a CMIPv6 session.
Expected Behaviour	Check that: when the IUT receives a Mobility Advertisement message with lifetime timer = 0, the IUT sends a binding update message using its current IP address and credentials and include a lifetime timer value of 0.
Test strategy	
Notes	

TP ID	TP/MS/CMIPv6/BV-H004
Reference	WFNA Stage2p2 [2]: section 7.8.2.5.5. WFNA Stage3 [3]: section 4.8.4.4.1. RFC 3775 [17].
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is currently involved in a CMIPv6 session.
Expected Behaviour	Check that: when the IUT decides to terminate the CMIPv6 session, the IUT sends a binding update message using its current IP address and credentials and include a lifetime timer value of 0.
Test strategy	
Notes	Requires means to cause the IUT to initiate session termination.

Sequence number in Binding Update

TP ID	TP/MS/CMIPv6/BV-H005
Reference	[3] WFNA Stage3: section 4.8.4 [17] RFC 3775 [17]: section 11.7.1
PICS Item	PIC_CMIPv6
Initial Condition	IUT has completed IPv6 Address assignment using either stateful or stateless IP configuration. The IUT has sent a Binding Update message with the Destination Option Header and mobility header (MH type 5).
Expected Behaviour	Check that: when the IUT receives a Binding Acknowledgement with status "Sequence number out of window", the IUT sends another Binding Update message with Sequence number parameter incremented by 1 compared to the previous Binding Update message.
Test strategy	
Notes	

Duplicate Address Detection behaviour

TP ID	TP/MS/CMIPv6/BV-H006
Reference	WFNA Stage3 [3]: section 4.8.4. RFC 3775 [17]: section 11.7.1.
PICS Item	PIC_CMIPv6.
Initial Condition	IUT has completed IPv6 Address assignment using stateless IP auto configuration, i.e. The IUT has sent a Binding Update message with the Destination Option Header and mobility header (MH type 5).
Expected Behaviour	Check that: when the IUT receives a Binding Acknowledgement with status "Dublicate Address Detection Failed", the IUT does not send the same Binding Update message again.
Test strategy	
Notes	

Return Routability Procedure

TP ID	TP/MS/CMIPv6/BV-H007
Reference	WFNA Stage2p2 [2]: section 7.8.2.14. WFNA Stage3 [3]: section 4.8.4. RFC 3775 [17]: section 5.2.5.
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is away from home and has been assigned a "care-of-address".
Expected Behaviour	Check that: The IUT sends a Home Test Init to the Home agent with parameter Source_address set to the Home_address and parameter Destination_address set to Correspondent_Node_address; and sends a Care-of Test Init message to the Correspondent node with parameter Source_address set to Care_of_address, parameter .Destination_address set to Correspondent_Node_address, and with a care_of_init_cookie.
Test strategy	
Notes	Requires a means to make the IUT initiate the Return Routability procedure.

TP ID	TP/MS/CMIPv6/BV-H008
Reference	WFNA Stage2p2 [2]: section 7.8.2.14. WFNA Stage3 [3]: section 4.8.4. RFC 3775 [17]: section 5.2.5.
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is away from home and has been assigned a "care-of-address" and has sent a Home_Test_Init and a Care_of_Test_Init message.
Expected Behaviour	Check that: When the IUT receives a Home_test message from Home_Agent containing source_address set to Correspondent_Node_address, Destination_address set to Home_address, and containing ESP_header, home_init_cookie, home_keygen_token, and home_nonce_index, and a Care_of_Test_Init message from Correspondent_Node containing source_address set to Correspondent_Node_address, destination_address set to care_of_address, and containing care_of_init_token, care_of_keygen_token, and care_of_nonce_index, the IUT sends a Binding Update message to the Correspondent Node.
Test strategy	
Notes	Requires a means to make the IUT initiate the Return Routability procedure.

TP ID	TP/MS/CMIPv6/BV-H009
Reference	WFNA Stage2p2 [2]: section 7.8.2.14. WFNA Stage3 [3]: section 4.8.4. RFC 3775 [17]: sections 5.2.5, 5.2.6 and 6.2.7.
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is away from home and has completed the Return Routability procedure and is to register its binding with the care-of-address.
Expected Behaviour	Check that: The IUT sends a Binding Update (BU) message to the correspondent Node with parameters source_address set to Care_of_Address, destination_address set to Correspondent_Node_address, nonce_indices_option set to Home_Nonce_Index, and Binding_Authorization_Data_option set to First(96, HMAC_SHA1(Kbn, (care-of-address | correspondent | BU)) where "care-of-address" is the care-of-address for the IUT if the BU is successful, "correspondent" is the IPv6 address of the correspondent node, and "BU" is the content of the BU message itself.
Test strategy	
Notes	Requires a means to make the IUT initiate the Return Routability procedure.

Mobility header processing

TP ID	TP/MS/CMIPv6/BV-H010
Reference	WFNA Stage2p2 [2]: section 7.8.2.14. WFNA Stage3 [3]: section 4.8.4. RFC 3775 [17]: sections 5.2.5, 6.1 and 9.2.
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is away from home and has been assigned a "care-of-address" and has sent a Home_Test_Init and a Care_of_Test_Init message.
Expected Behaviour	Check that: When the IUT receives a Home Test message with an incorrect checksum, the IUT ignores the Home Test message.
Test strategy	
Notes	Requires a means to make the IUT initiate the Return Routability procedure.

TP ID	TP/MS/CMIPv6/BV-H011
Reference	WFNA Stage2p2 [2]: section 7.8.2.14. WFNA Stage3 [3]: section 4.8.4. RFC 3775 [17]: sections 5.2.5, 6.1 and 9.2.
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is away from home and has been assigned a "care-of-address" and has sent a Home_Test_Init and a Care-of Test Init message.
Expected Behaviour	Check that: When the IUT receives a Care-of Test message with an incorrect checksum, the IUT ignores the Care-of Test message.
Test strategy	
Notes	Requires a means to make the IUT initiate the Return Routability procedure.

TP ID	TP/MS/CMIPv6/BV-H012
Reference	WFNA Stage2p2 [2]: section 7.8.2.14. WFNA Stage3 [3]: section 4.8.4. RFC 3775 [17]: sections 5.2.5, 6.1 and 9.2.
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is away from home and has been assigned a "care-of-address" and has sent a Home_Test_Init and a Care-of Test Init message.
Expected Behaviour	Check that: When the IUT receives a Home Test message with parameter payload_proto_field set to a value different to 59, the IUT ignores the Home Test message and optionally sends a ICMP_Parametter_Problem message with parameter code set to 0 (Erroneous header filed encountered) and with pointer indicating Payload_proto_field.
Test strategy	
Notes	Requires a means to make the IUT initiate the Return Routability procedure.

TP ID	TP/MS/CMIPv6/BV-H013
Reference	WFNA Stage2p2 [2]: section 7.8.2.14. WFNA Stage3 [3]: section 4.8.4. RFC 3775 [17]: sections 5.2.5, 6.1 and 9.2.
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is away from home and has been assigned a "care-of-address" and has sent a Home_Test_Init and a Care-of Test Init message.
Expected Behaviour	Check that: When the IUT receives a Care-of Test message with parameter payload_proto_field set to a value different to 59, the IUT ignores the Care-of Test message and optionally sends a ICMP_Parametter_Problem message with parameter code set to 0 (Erroneous header filed encountered) and with pointer indicating Payload_proto_field.
Test strategy	
Notes	Requires a means to make the IUT initiate the Return Routability procedure.

TP ID	TP/MS/CMIPv6/BV-H014
Reference	WFNA Stage2p2 [2]: section 7.8.2.14. WFNA Stage3 [3]: section 4.8.4. RFC 3775 [17]: sections 5.2.5, 6.1 and 9.2.
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is away from home and has been assigned a "care-of-address" and has sent a Home_Test_Init and a Care-of Test Init message.
Expected Behaviour	Check that: When the IUT receives a Home Test message with a header_length_field less than the required length, the IUT ignores the Home Test message and optionally sends an ICMP_Parametter_Problem message with parameter code set to 0 (Erroneous header filed encountered) and with pointer indicating Header_length_field.
Test strategy	
Notes	Requires a means to make the IUT initiate the Return Routability procedure.

TP ID	TP/MS/CMIPv6/BV-H015
Reference	WFNA Stage2p2 [2]: section 7.8.2.14. WFNA Stage3 [3]: section 4.8.4. RFC 3775 [17]: sections 5.2.5, 6.1 and 9.2.
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is away from home and has been assigned a "care-of-address" and has sent a Home_Test_Init and a Care-of Test Init message.
Expected Behaviour	Check that: When the IUT receives a Care-of Test message with a header_length_field less than the required length, the IUT ignores the Care-of Test message and optionally sends a ICMP_Parametter_Problem message with parameter code set to 0 (Erroneous header filed encountered) and with pointer indicating Header_length_field.
Test strategy	
Notes	Requires a means to make the IUT initiate the Return Routability procedure.

Binding refresh reception shall cause transmission of a Binding Update

TP ID	TP/MS/CMIPv6/BV-H015
Reference	WFNA Stage2p2 [2]: section 7.8.2.14. WFNA Stage3 [3]: section 4.8.4. RFC 3775 [17]: sections 6.1.2 and 8.5.
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is currently involved in a CMIPv6 session.
Expected Behaviour	Check that: When the IUT receives a Binding Update Refresh message, the IUT send a Binding Update message.
Test strategy	
Notes	

Binding error message

TP ID	TP/MS/CMIPv6/BV-H016
Reference	WFNA Stage3 [3]: section 4.8.4. RFC 3775 [17]: section 11.3.6.
PICS Item	PIC_CMIPv6.
Initial Condition	The IUT is currently involved in a CMIPv6 session and an ongoing packet exchange to correspondent node, but the IUT has no upper layer information on the progress of this packet exchange.
Expected Behaviour	Check that: When the IUT receives a Binding Error message with status set to 1 "unknown binding for Home Address destination", the IUT stop the packet exchange to the correspondent node and may initiate return routability procedure, by sending a Home Test Init and Care-of Test Init message.
Test strategy	
Notes	

Annex A (informative): Bibliography

- IEEE 802.3: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications".
- ISO 3166: "Codes for the representation of names of countries and their subdivisions".
- ETSI TS 102 545-2 (V1.1.1): "Broadband Radio Access Networks (BRAN); HiperMAN; Conformance Testing for WiMAX/HiperMAN 1.3.1; Part 2: Test Suite Structure and Test Purposes (TSS&TP)".
- ETSI TS 102 545-1 (V1.1.1): "Broadband Radio Access Networks (BRAN); HiperMAN; Conformance Testing for WiMAX/HiperMAN 1.3.1; Part 1: Protocol Implementation Conformance Statement (PICS) proforma".
- WiMAX Forum: Mobile System Profile Release 1.0.

History

Document history		
V1.1.1	October 2008	Publication