ETSI TS 102 624-2 V1.2.1 (2009-11)

Technical Specification

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

Reference

RTS/BRAN-004T010-2

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

Individual copies of the present document can be downloaded from:

http://www.etsi.org

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

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

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

Copyright Notification

ETSI

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Broadband Radio Access Networks (BRAN).

The present document specifies the Test Suite Structure and Test Purposes (TSS&TP) of the Network layer Release 1.5 for High Performance radio Metropolitan Area Network (HiperMAN) and WiMAX terminal devices.

The present document is part 2 of a multi-part deliverable covering HiperMAN; Conformance Testing for the Network Layer of HiperMAN/WiMAX terminal devices, as identified below:

Part 1:   "Protocol Implementation Conformance Statement (PICS) proforma";

Part 2:   "Test Suite Structure and Test Purposes (TSS&TP)";

Part 3:   "Abstract Test Suite (ATS)".

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 Release 1.5.

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.

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 (Release 1.5): "WiMAX Forum Network Architecture, Stage 2: Architecture Tenets, Reference Model and Reference Points, Base Specification".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release.

[2]   WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture, Stage 3: Detailed Protocols and Procedures, Base Specification".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release.

[3]   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".

[4]   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.

[5]   IETF RFC 791 (September 1981): "Internet Protocol".

[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]   Void.

[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)".

[26]   WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Stage 3: Architecture,
            detailed Protocols and Procedures: WiMAX Over-The-Air General Provisioning System
            Specification".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release.

[27]   WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Stage 3: Architecture,
            detailed Protocols and Procedures: Over-The-Air Provisioning & Activation Protocol based on
            TR-069 Specification".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release.

[28] WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Stage 3: Architecture, detailed Protocols and Procedures; WiMAX Over-The-Air Provisioning & Activation Protocol based on OMA DM Specifications".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release.

[29] WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Stage 3: Architecture, detailed Protocols and Procedures; Emergency Services Support".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release.

[30] WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Stage 3: Architecture, detailed Protocols and Procedures; IP Multimedia Subsystem (IMS) Interworking".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release.

[31] WiMAX Forum (Release 1.5): "WiMAX Forum Network Architecture; Protocol and Procedures for Location Based Services".

NOTE: Available at http://www.wimaxforum.org/resources/documents/technical/release.

[32] Void.

[33] IETF RFC 2782 (February 2000): "A DNS RR for specifying the location of services (DNS SRV)".

[34] IETF RFC 2616 (June 1999): "Hypertext Transfer Protocol -- HTTP/1.1".

[35] Open Mobile Alliance OMA-TS-DM-Protocol-V1-2-20070209-A (February 2007) (V1.2): "OMA Device Management Protocol".

[36] Broadband Forum (December 2007, Issue 1 Amnd. 2): "TR-069; CPE WAN Management Protocol v1.1".

[37] IETF RFC 5031 (January 2008): "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services".

[38] Void.

[39] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229 Release 7)".

[40] IETF RFC 4282 (December 2005): "The Network Access Identifier".

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

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.

[i.1] ETSI TS 102 624-3: "Broadband Radio Access Networks (BRAN); HiperMAN; Conformance Testing for the Network layer of HiperMAN/WiMAX terminal devices; Part 3: Abstract Test Suite (ATS)".

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 [41] and IEEE 802.16e [4] 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 [41], IEEE 802.16e [4] and the following apply:

AKA	Authentication and Key Agreement
AVP	Attribute Value Pair
BI	Invalid Behaviour
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
TI	Timer
TLS	Transport Layer Security
TP	Test Purposes
TSS	Test Suite Structure
TTLS	Tunneled Transport Layer Security
UL	Uplink

4   Test Suite Structure (TSS)

4.1   Structure

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

Group	Function	Sub-function
Network Entry		
Client DHCPv4		
Client MIP v4 mobility management		
IPv4 Transport		
Security		

Group	Function	Sub-function
	Device authentication (EAP-TLS)	
		Fragmentation
	User authentication (EAP-AKA)	
	User authentication (EAP-TTLSv0)	
		Fragmentation
	CMAC Keys	
	EAP-TTLSv0/MS-CHAP-v02	
IPv6 Transport		
Client MIP v6 mobility management		
OTA Provisioning and Activation		
	OMA	
		Bootstrap
		Provisioning
	TR-069 based	
		Bootstrap
		Provisioning
Emergency Services		
Location Based Services		
IP-IMS Interworking		

Figure 1: TSS for WiMAX Forum Network architecture

The test suite is structured as a tree with the root defined as MS representing the "Network architecture protocols 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).

4.2   Test groups

Each test group has up to a maximum 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 category of the test of the test purpose. This fourth level is not shown in figure 1.

4.2.1   Protocol services

The protocol groups identify the Network Layer protocol services defined in WiMAX Forum Network Architecture [1], and [2] relevant for MS.

4.2.1.1   Network Discovery and Selection (NWE)

This test group contains test purposes for MS detection and selection of network service provider.

4.2.1.2   Proxy MIPv4 (DHCP)

This test group contains test purposes for MS Proxy MIPv4 behaviour (DHCP) including address acquisition, and address renewal.

4.2.1.3   Client MIPv4 (CMIPv4)

This test group contains test purposes for MS Client MIPv4 behaviour (CMIPv4) including registration, re-registration, session termination, and mobility management.

4.2.1.4   IPv4 Transport (IPv4)

This test group contains test purposes for specific IPv4 requirements (Fragmentation) defined in the Network Architecture.

4.2.1.5 Security (SEC)

This test group contains test purposes for MS authentication procedures, device and user authentication.

4.2.1.6 Client MIPv6 (CMIPv6)

This test group contains test purposes for MS Client MIPv6 (CMIPv6) procedures including registration, handover, session renewal, and termination.

4.2.1.7 IPv6 Transport (IPv6)

This test group contains test purposes for MS IPv6 address management, including acquisition, renewal, and fragmentation.

4.2.1.8 Over-The-Air (OTA) Provisioning and Activation

This test group contains test purposes for OTA MS management procedures based on either OMA or TR-069protocols.

4.2.1.9 Emergency Services

This test group contains test purposes for MS Emergency Service functions.

4.2.1.10 Location Based Services

This test group contains test purposes for MS Location Based Service functions.

4.2.1.11 IP-IMS interworking

This test group contains test purposes for MS interworking with IP-IMS services.

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>	Name	Functionality
	<st> = side type	MS	Mobile Station
	<pg> = protocol group	NWE	Network Discovery and Selection
		CMIPv4	Client Mobile IP v4 mobility management
		IPv4	IP v4
		DHCP	Dynamic Host Configuration Protocol (PMIP4)
		SEC	Security
		IPv6	IP v6
		CMIPv6	Client Mobile IP v6 mobility management
		OTA	Over-The-Air Provisioning and Activation
		EMG	Emergency Services
		LBS	Location Based Services
		IMS	IP-IMS Interworking
	<fg> = function group		
		EAPTLS	Extensible Authentication Protocol - Transport Level Security
		EAPTTLSv0	Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0
		EAPAKA	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement
		OMA	Open Mobile Alliance protocols
		T69	Broadband Forum TR-069 protocols
	<sg> = subfunction group		
		BTS	Bootstrap
		PVS	Provisioning and Activation
	<x> = type of testing		
		BV	Valid Behavior
		TI	Timer Behavior
		BI	Invalid Behavior
	<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] and [2].

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 [3]	Criteria
1	PIC_MNS	A.3/1	MS supports Manual NSP selection
2	PIC_ANS	A.32	MS supports Automatic NSP selection
3	PIC_CMIPV4	A.9/2	MS supports CMIPv4
4	PIC_EAPAKA	A.6/1	MS supports EAP-AKA user authentication.
5	PIC_EAPTTLS	A.6/2	MS supports EAP-TTLS user authentication.
6	PIC_DHCPv4	A.9/1	MS supports DHCP V4
7	PIC_DHCPv4_RA	A.12/2	MS supports re-use of assigned address
9	PIC_RRRTM	A.13/5	MS supports Registration Request re-transmission
10	PIC_SAA	A.19/6	MS supports Stateful Address Autoconfiguration (DHCPv6)
11	PIC_IP6	A.1/4	MS supports IPv6
12	PIC_RELEASE	A.20/7	MS supports sending of message DHCPRELEASE
13	PIC_CMIPv6	A.15/2	MS supports CMIP6 mobility management
14	PIC_OTA	A.1/5	MS supports OTA provisioning and activation
15	PIC_TR069	A.22/2 or A.23/2 or A.24/2	OTA MS supports OTA TR-069 based provisioning and activation
16	PIC_OMA	A.22/1 or A.23/1 or A.24/1	OTA MS supports OTA OMA based provisioning and activation
17	PIC_TPA	A.20/1	OTA MS is of type Model A
18	PIC_TPB1	A.20/2	OTA MS is of type Model B1
19	PIC_TPB2	A20/3	OTA MS is of type Model B2
20	PIC_SIB	A.26/1	OTA MS (Model B) supports OMA server initiated bootstrap
21	PIC_LO	A.29/2	OTA OMA MS supports Large Objects
22	PIC_CM	A.30/2	OTA OMA MS supports client initiated polling for Continuous Management
23	PIC_EMG_VOIP	A.32/1	Support for VoIP service
24	PIC_EMG_RCG	A.32/2	MS recognizes Emergency Service calls
25	PIC_EMG_SIP	A.33/1	MS uses SIP in the VoIP Service
26	PIC_WLPN	A.35/3	MS supports WiMAX Location Protocol (WLP) negotiation
27	PIC_AGPS	A32/3	MS supports Assisted GPS
28	PIC_SUPL	A.34/2	MS supports OMA Secure User Plane Location (SUPL)
29	PIC_IMS	A.1/7	MS supports IP-IMS interworking
30	PIC_WIB	A.28/2	MS supports Initial Bootstrap procedure

5.2   Test purposes for MS

5.2.1   Network entry (Discovery and Selection)

Manual selection mode

TP ID	TP/MS/NWE/BV-H000
Reference	WFNA Stage3 [2]: section 4.1.2.3.1.
PICS Item	PIC_MNS
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. MS is in unactivated state.
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	The IUT requests list in the SBC-REQ with the SIQ-TLV set to 1,1 the SBC-RSP provides the NSP ID, and Verbose NSPID for each available NSP. The IUT transmits an EAP-Response/Identity containing a NAI with the selected NSP as the realm which must correspond to the manually selected NSP.
Notes	Requires operator intervention in the IUT.

TP ID	TP/MS/NWE/BV-H001
	Deleted.

TP ID	TP/MS/NWE/BV-H002
Reference	[2] WFNA Stage3: sections 4.1.2.2 and 4.1.2.3.1
PICS Item	PIC_MNS
Initial Condition	The IUT is attempting network re-entry either with previous cached NAP/NSP configuration information available or by performing Network Discovery and the IUT operates in manual NSP selection mode. NSP Change Count TLV in the DCD messages sent by the TE is unchanged from initial network entry.
Expected Behaviour	Check that: When the IUT has performed network discovery the IUT presents the available NSPs enumeration list.
Test strategy	
Notes	Requires operator intervention in the IUT. . If the NSP Change Count TLV is unchanged, the IUT might still query the info, as example if it has returned to defaults and possibly due to other reasons

TP ID	TP/MS/NWE/BV-H002a
Reference	[2] WFNA Stage3: sections 4.1.2.2 and 4.1.2.3.1
PICS Item	PIC_MNS
Initial Condition	The IUT is attempting network re-entry. NSP Change Count TLV in the DCD messages sent by the TE is changed from initial network entry.
Expected Behaviour	Check that: When the IUT performs network discovery and presents the newly obtained NSPs enumeration list.
Test strategy	
Notes	Requires operator intervention in the IUT.

Automatic selection mode

TP ID	TP/MS/NWE/BV-H003
Reference	[2] WFNA Stage3: sections 4.1.2.3.2
PICS Item	PIC_ANS
Initial Condition	The IUT is attempting initial network entry using automatic mode without user intervention and more NSPs are available including the Home NSP. The IUT has no stored NAP/NSP configuration available.
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	The TE in the SII-ADV or on request in the SBC-RSP indicates the NSP ID for each available NSP among which is the Home NSP of the IUT. In automatic mode the IUT transmits an EAP-Response/Identity containing a NAI with the home NSP realm during initialization.
Notes	

TP ID	TP/MS/NWE/BV-H004
Reference	[2] WFNA Stage3: section 4.1.2.3.2
PICS Item	PIC_ANS
Initial Condition	The IUT is attempting network entry using automatic mode without user intervention. The IUT has previously stored NAP/NSP configuration available. During the network discovery procedure the Home NSP is available as a new available NSP option.
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	In automatic mode the IUT transmits an EAP-Response/Identity containing a NAI with the home NSP realm during this network entry.
Notes	Requires an upper tester. It is checked that the IUT uses the stored configuration information if the IUT does not send any RNG-REQ or SBC-REQ during network discovery. It requires that the NSP Change Count TLV in the DCD messages sent by the TE is unchanged from initial network entry.

Selection mode (manual/automatic) independent TPs

TP ID	TP/MS/NWE/BV-H005
Reference	[2] WFNA Stage3: section 4.1.2.2
PICS Item	
Initial Condition	The IUT is attempting initial network entry without NAP/NSP configuration information and the TE sends DL-MAPs with NAPID's NSP Identifier Flag=1 and the TE does not send SII-ADV messages.
Expected Behaviour	Check that: When the IUT performs NSP discovery procedure the IUT sends a SBC-REQ message with SIQ TLV with bit 0 set to '1'.
Test strategy	
Notes	

TP ID	TP/MS/NWE/BV-H006
Reference	[2] WFNA Stage3: section 4.1.2.2
PICS Item	
Initial Condition	The IUT has performed network discovery.
Expected Behaviour	Check that: When the IUT performs network entry with a selected BS, the IUT does not include the SIQ TLV in the SBC-REQ that it sends.
Test strategy	
Notes	

5.2.2   DHCP group

TP ID	TP/MS/DHCP/BV-H000
Reference	WFNA Stage2p2 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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	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].
Test strategy	
Notes	

TP ID	TP/MS/DHCP/BV-H001
Reference	WFNA Stage2p2 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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 sends a new DHCPDISCOVER message.
Test strategy	
Notes	

TP ID	TP/MS/DHCP/BV-H008
Reference	WFNA Stage2p2 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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 sends a new DHCPDISCOVER message.
Test strategy	
Notes	

TP ID	TP/MS/DHCP/BV-H009
Reference	WFNA Stage2p2 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: section 4.8.2.1.1. RFC 2131 [8]: section 4.4.6.
PICS Item	PIC_DHCPv4 AND PIC_RELEASE.
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.

TP ID	TP/MS/DHCP/BV-H011
Reference	WFNA Stage2p2 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: section 4.8.2.1.2.1, 4.8.2.1.7.1. RFC 2131 [8]: section 3.2.
PICS Item	PIC_DHCPv4 and PIC_DHCPv4_RA.
Initial Condition	The MS has been assigned a network address (PoA).
Expected Behavior	Check that: when the link is lost and the IUT recovers using scan, connect, and network entry, the IUT sends a DHCPREQUEST containing the previously assigned network address in the optional Requested IP Address field.
Test strategy	
Notes	Requires that the IUT uses the abbreviated address allocation procedure, [8]: section 3.2.

5.2.2.1   DHCP timer

TP ID	TP/MS/DHCP/TI-H000
Reference	WFNA Stage2p2 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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 [1]: sections 7.2.1.3 and 7.8.1.8. WFNA Stage3 [2]: 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 [1]: section 7.8.1.9.1. WFNA Stage3 [2]: section 4.8.3.1. RFC 3344 [10].
PICS Item	PIC_CMIPV4.
Initial Condition	The MS has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of MS flow to intra-ASN data path as shown in stage2 figure 7-70 step 2 is complete. The MS will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The MS has the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage3 section 4.3.1]. The MS has the out NAI (bootstrapped during normal authentication phase) [See Stage3 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 generates and sends a MIPv4 registration request message to the foreign agent with the HA field set to 255.255.255.255.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H001
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.1. WFNA Stage3 [2]: section 4.8.3.1. RFC 3344 [10].
PICS Item	PIC_CMIPV4.
Initial Condition	The MS has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of MS flow to intra-ASN data path as shown in stage2 figure 7-70 step 2 is complete. The MS will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The MS has the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage3 section 4.3.1]. The MS has the out NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The IUT is provisioned with the HA address. 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 has access to the HA address.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H002
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.2. WFNA Stage3 [2]: 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 MIPv4 re-Registration Reply based on the IUT MIPv4 Registration Request. The IUT has the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5], the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage3 section 4.3.1], and the out NAI (bootstrapped during normal authentication phase) [See Stage3 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 contain the Home Address field set to the home address, the Home Agent field set to the home agent address, and the NAI extension field to the value "Identity@realm" that was used during the authentication process. The request shall also include the MN-HA authentication extension and may include the MN-FA authentication extension.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H003
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.5. WFNA Stage3 [2]: 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 MIPv4 Registration Reply based on the MIPv4 Registration Request received from the IUT. The IUT has the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5], the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage3 section 4.3.1], and the out NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1].
Expected Behaviour	Check that 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	Requires a means to cause the IUT to initiate session termination e.g. perform a gracefully shut down.

TP ID	TP/MS/CMIPV4/BV-H004
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.3. WFNA Stage3 [2]: 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 containing a different CoA the IUT sends a MIPv4 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 [1]: section 7.8.1.9.3. WFNA Stage3 [2]: 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 Stage2 figure 7-70 step 1. Binding of MS flow to intra-ASN data path as shown in stage2 figure 7-70 step 2 is complete. The MS will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The MS has the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage3 section 4.3.1]. The MS has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 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 [1]: section 7.8.1.9.3. WFNA Stage3 [2]: 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 Stage2 figure 7-70 step 1. Binding of MS flow to intra-ASN data path as shown in stage2 figure 7-70 step 2 is complete. The MS will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The MS has the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage3 section 4.3.1]. The MS has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 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	The TE does not respond to received Agent Solicitation messages.

TP ID	TP/MS/CMIPV4/BV-H007
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.3. WFNA Stage3 [2]: 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 Stage2 figure 7-70 step 1. Binding of MS flow to intra-ASN data path as shown in stage2 figure 7-70 step 2 is complete. The MS will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The MS has the CMIPv4 SPI (bootstrapped during normal authentication phase) [see Stage3 section 4.3.1]. The MS has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 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	The TE does not respond to received Agent Solicitation messages.

TP ID	TP/MS/CMIPV4/BV-H008
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.1. WFNA Stage3 [2]: section 4.8.3.1. RFC 3344 [10].
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of IUT flow to intra-ASN data path as shown in Stage2 figure 7-70 step 2 is complete. The IUT will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The IUT has the CMIPv4 SPI (bootstrapped during normal authentication phase) [See Stage3 section 4.3.1]. The IUT has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The Network has sent a Mobile IP Agent Advertisement message to the IUT that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10] section 2.1.
Expected Behaviour	Check that: if the IUT desires to use dynamic home address assignment for the initial registration, the IUT shall generate and send a MIPv4 Registration Request message to the foreign agent with the Home address (HoA) field set to 0.0.0.0 to indicate dynamic HA assignment.
Test strategy	
Notes	Requires a means to make the IUT use dynamic home address assignment

TP ID	TP/MS/CMIPV4/BV-H009
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.1. WFNA Stage3 [2]: section 4.8.3.1. RFC 3344 [10].
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of IUT flow to intra-ASN data path as shown in Stage2 figure 7-70 step 2 is complete. The IUT will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The IUT has the CMIPv4 SPI (bootstrapped during normal authentication phase) [See Stage3 section 4.3.1]. The IUT has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The Network has sent a Mobile IP Agent Advertisement message to the IUT that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10] section 2.1.
Expected Behaviour	Check that: if the IUT uses static home address assignment for the initial registration, the IUT sends the MIPv4 Registration Request message to the foreign agent with the Home address (HoA) field set to its home address.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H010
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.1. WFNA Stage3 [2]: section 4.8.3.1. RFC 3344 [10]: sections 3.5.2 and 3.5.3
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of IUT flow to intra-ASN data path as shown in Stage2 figure 7-70 step 2 is complete. The IUT will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The IUT has the CMIPv4 SPI (bootstrapped during normal authentication phase) [See Stage3 section 4.3.1]. The IUT has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The Network has sent a Mobile IP Agent Advertisement message to the IUT that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10] section 2.1.
Expected Behaviour	Check that: when the IUT generates and sends a MIPv4 initial Registration Request message to the foreign agent the registration request message shall contain a Mobile Node Home Agent (MN-HA) authentication extension and may contain a Mobile Node Foreign Agent (MN-FA) authentication extension.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H011
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.1. WFNA Stage3 [2]: section 4.8.3.1. RFC 3344 [10]: section 3.6.
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of IUT flow to intra-ASN data path as shown in Stage2 figure 7-70 step 2 is complete. The IUT will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The IUT has the CMIPv4 SPI (bootstrapped during normal authentication phase) [See Stage3 section 4.3.1]. The IUT has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The Network has sent a Mobile IP Agent Advertisement message to the IUT that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10] section 2.1.
Expected Behaviour	Check that: when the IUT generates and sends a MIPv4 initial Registration Request message to the foreign agent the registration request message shall contain a NAI extension with the value "Identity@realm" that was used during the authentication process.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H012
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.1. WFNA Stage3 [2]: section 4.8.3.1.1. RFC 3344 [10].
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of IUT flow to intra-ASN data path as shown in Stage2 figure 7-70 step 2 is complete. The IUT will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The IUT has the CMIPv4 SPI (bootstrapped during normal authentication phase) [See Stage3 section 4.3.1]. The IUT has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The Network has sent a Mobile IP Agent Advertisement message to the IUT that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10] section 2.1. The IUT has sent a Registration Request message indicating static Home Address (HoA) assignment and dynamic Home Agent assignment (HA field set to either 255.255.255.255 or 0.0.0.0).
Expected Behaviour	Check that: when the IUT receives a Registration Reply message indicating successful registration containing a different HoA, the IUT uses the received HoA in the mobile session.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H013
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.1. WFNA Stage3 [2]: section 4.8.3.1.1. RFC 3344 [10]: section 3.6.1.1
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of IUT flow to intra-ASN data path as shown in Stage2 figure 7-70 step 2 is complete. The IUT will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The IUT has the CMIPv4 SPI (bootstrapped during normal authentication phase) [Stage3 section 4.3.1]. The IUT has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The Network has sent a Mobile IP Agent Advertisement message to the IUT that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10] section 2.1.
Expected Behaviour	Check that: when the IUT generates and sends a MIPv4 Registration Request message to the foreign agent the message contains the IP Destination Address field set to the value of the IP Source Address of the received Agent Advertisement message.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H014
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.1. WFNA Stage3 [2]: section 4.8.3. RFC 3344 [10]: section 4.4.1.
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of IUT flow to intra-ASN data path as shown in Stage2 figure 7-70 step 2 is complete. The IUT will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The IUT has the CMIPv4 SPI (bootstrapped during normal authentication phase) [See Stage3 section 4.3.1]. The IUT has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The Network has sent a Mobile IP Agent Advertisement message to the IUT that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10] section 2.1.
Expected Behaviour	Check that: when the IUT generates and sends a MIPv4 Registration Request message to the foreign agent to request a registration with a reverse tunnel the Request message has the set the 'T' bit to 1 and the TTL field of the IP header to 255.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H015
Reference	WFNA Stage3 [2]: section 4.8.3. RFC 3344 [10]: section 4.4.
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of IUT flow to intra-ASN data path as shown in Stage2 figure 7-70 step 2 is complete. The IUT will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The IUT has the CMIPv4 SPI (bootstrapped during normal authentication phase) [See Stage3 section 4.3.1]. The IUT has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The Network has sent a Mobile IP Agent Advertisement message to the IUT that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10] section 2.1. The IUT has sent a Registration Request with request for reverse tunnelling and has received a Registration Reply indicating successful registration.
Expected Behaviour	Check that: when IUT generates and sends a datagram to a multicast address the IUT uses its home address as the IP source address of both the inner multicast diagram and the outer encapsulating datagram.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H016
Reference	WFNA Stage2p2 [1]: section 7.8.1.9.1. WFNA Stage3 [2]: section 4.8.3. RFC 3344 [10]: section 4.4.
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of IUT flow to intra-ASN data path as shown in Stage2 figure 7-70 step 2 is complete. The IUT will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The IUT has the CMIPv4 SPI (bootstrapped during normal authentication phase) [See Stage3 section 4.3.1]. The IUT has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The Network has sent a Mobile IP Agent Advertisement message to the IUT that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10] section 2.1. The IUT has sent a Registration Request.
Expected Behaviour	Check that: when the IT receives Registration Reply indicating successful registration and containing a remaining Lifetime field with a value lower than requested in the Registration Request, the IUT uses this as the remaining lifetime value before performing registration renewal procedure.
Test strategy	
Notes	

Registration Re-Transmissions

TP ID	TP/MS/CMIPV4/BV-H017
Reference	WFNA Stage3 [2]: section 4.8.3. RFC 3344 [10]: sections 3.6.3 and 4.4.
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of IUT flow to intra-ASN data path as shown in Stage2 figure 7-70 step 2 is complete. The IUT will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The IUT has the CMIPv4 SPI (bootstrapped during normal authentication phase) [See Stage3 section 4.3.1]. The IUT has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The Network (TE) has sent a Mobile IP Agent Advertisement message to the IUT that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10] section 2.1. The IUT has sent a Registration Request using timestamp in the Identification field.
Expected Behaviour	Check that: when the IUT does not receive a Registration Reply in response to the Registration Request it sends another Registration Request with an updated timestamp, but not until at least 1 second after the first Registration Request was sent.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BV-H018
Reference	WFNA Stage3 [2]: section 4.8.3. RFC 3344 [10]: section 3.6.3.
PICS Item	PIC_CMIPV4 AND PIC_RRRTM
Initial Condition	The IUT has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of IUT flow to intra-ASN data path as shown in Styage-2 figure 7-70 step 2 is complete. The IUT will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The IUT has the CMIPv4 SPI (bootstrapped during normal authentication phase) [See Stage3 section 4.3.1]. The IUT has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The Network (TE) has sent a Mobile IP Agent Advertisement message to the IUT that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10] section 2.1. The IUT has sent a Registration Request using timestamp in the Identification field.
Expected Behaviour	Check that: when the IUT does not receive a Registration Reply in response to a Registration Request it sends successive Registration Requests with updated timestamps with time intervals between transmissions that are at least twice the previous time interval but less than the requested Lifetime in the Registration Request.
Test strategy	
Notes	

Handover

TP ID	TP/MS/CMIPV4/BV-H019
Reference	WFNA Stage3 [2]: section 4.8.3.3.1. RFC 3344 [10]: section 3.3.
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 MIPv4 Registration Reply based on the IUT MIPv4 Registration Request.
Expected Behaviour	Check that: When in connection with a CSN anchored mobility handover the IUT receives an Agent Advertisement message with a new Foreign Agent Care of Address (FA-CoA) the IUT sends a Registration Request message to this FA.
Test strategy	
Notes	

Termination

TP ID	TP/MS/CMIPV4/BV-H020
Reference	WFNA Stage3 [2]: section 4.8.3.4. RFC 3344 [10]: section 2.1.
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 MIPv4 Registration Reply based on the IUT MIPv4 Registration Request.
Expected Behaviour	Check that: When the IUT receives an Agent Advertisement message from the Foreign Agent (FA) that the IUT is currently registered with and that this message has the busy bit 'B' set the IUT shall consider the session terminated and shall not try to register with this Foreign Agent until it receives another Agent Advertisement from the same FA where the 'B' bit is not set.
Test strategy	
Notes	

TP ID	TP/MS/CMIPV4/BI-H000
Reference	WFNA Stage2p2 [1]. WFNA Stage3 [2]: section 4.8.3.1.1. RFC 3344 [10]: section 1.8.
PICS Item	PIC_CMIPV4
Initial Condition	The IUT has completed the authentication process shown in Stage2 figure 7-70 step 1. Binding of IUT flow to intra-ASN data path as shown in Stage2 figure 7-70 step 2 is complete. The IUT will have the MN-HA Key (bootstrapped during normal authentication phase) [See Stage3 section 4.3.5]. The IUT has the CMIPv4 SPI (bootstrapped during normal authentication phase) [See Stage3 section 4.3.1]. The IUT has the outer NAI (bootstrapped during normal authentication phase) [See Stage3 section 4.4.1.3.1]. The Network (TE) has sent a Mobile IP Agent Advertisement message to the IUT that includes Care of Address for the foreign agent (CoA) per RFC 3344 [10] section 2.1. The IUT has sent a valid MIPv4 Registration Request message.
Expected Behaviour	Check that: when the IUT receives a MIPv4 Registration Reply containing a Mobile IP Extension structure numbered in the range from 128 to 255 not recognized by the IUT, the IUT ignores the Extension but otherwise processes the message.
Test strategy	
Notes	

5.2.4 IPv4

TP ID	TP/MS/IPv4/BV-H000
Reference	[WFNA Stage3 [2]: section 3.3.3, 4.2. RFC 791 [5].
PICS Item	
Initial Condition	IUT has completed set-up of IPv4 Initial Service Flow.
Expected Behaviour	Check that: when the IUT sends an UL IPv4 packet via the IPv4 Initial Service Flow exceeding the MTU size of 1400 bytes, the IPv4 packet is fragmented into more messages.
Test strategy	
Notes	Requires a means to make the IUT transmit an IPv4 packet exceeding the MTU size.

TP ID	TP/MS/IPv4/BV-H001
Reference	WFNA Stage3 [2]: sections 3.3.3 and 4.2. RFC 791 [5].
PICS Item	
PICS Item	
Initial Condition	IUT has completed set-up of IPv4 Initial Service Flow.
Expected Behaviour	Check that: the IUT correctly receives IPv4 packets via the IPv4 Initial Service Flow which have been fragmented due to the size exceeding MTU size of 1400 bytes.
Test strategy	

5.2.5 Security

	TP/MS/SEC/BV-H000
	Deleted

TP ID	TP/MS/SEC/BV-H001
Reference	WFNA Stage3 [2]: section 4.4.1.4.1.1.
PICS Item	
Initial Condition	The IUT is performing initialization and is entering Authorization phase. The IUT has a pre-provisioned realm.
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 [2]: 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. 4) IUT is pre-provisioned with a realm
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 [2]).

TP ID	TP/MS/SEC/EAPTLS/BV-H001
Reference	RFC 5216 [7]: section 3.1. WFNA Stage3 [2]: 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 2. WFNA Stage3 [2]: 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, 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 (1 400 B). See the section 4.4.1.2.1 of NWG Stage 3.

TP ID	TP/MS/SEC/EAPTLS/BV-H002a
Reference	RFC 5216 [7]: section 2.1.3 WFNA Stage3 [2]: section 4.4.1.2.1.
PICS Item	
Initial Condition	1) The TE has its own invalid 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, invalid TLS certificate, TLS certificate_request, TLS server_hello_done, the IUT terminates the authentication process and may respond with an EAP-Response/EAP-Type=EAP-TLS message containing a TLS Alert.
Test strategy	
Notes	Note that the EAP-TLS message MUST be fragmented if the message size is greater than MTU size (1 400 B). See the section 4.4.1.2.1 of NWG Stage 3.

TP ID	TP/MS/SEC/EAPTLS/BV-H003
Reference	RFC 5216 [7]. WFNA Stage3 [2]: 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 certificate", "TLS client_key_exchange", "TLS certificate_verify", "TLS change_cipher_spec", and "TLS finished" parameters in response to an EAP-Request/EAP-Type=EAP TLS with "TLS server_hello", "TLS certificate", "TLS server_key_exchange", "TLS certificate_request", 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   Retransmission behaviour

TP ID	TP/MS/SEC/EAPTLS/BV-H004
Reference	RFC 5216 [7]: section 3.2. WFNA Stage3 [2]: 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 and the same Identifier field value as in the previously sent EAP-Response.
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 [2]: 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 2.1.5. WFNA Stage3 [2]: 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 [2]: 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 [2]: 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 [2]: 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 [2]: 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 [2]: 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 [2]: 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 [2]: 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	RFC 5281 [12]. WFNA Stage3 [2]: 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	RFC 5281 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [2]: 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	RFC 5281 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [2]: 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-TTLS 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 (1 400 B). See the section 4.4.1.2.3 of NWG Stage 3.

TP ID	TP/MS/SEC/EAPTTLSv0/BV-H003
Reference	RFC 5281 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [2]: 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 "Certificate", "ClientExchange", "CertificateVerify", "ChangeCipherSpec", and "Finished" parameters and then received an EAP-Request with "ChangeCipherSpec" and "Finished" parameters.
Expected Behaviour	Check that: The IUT responds to the EAP-Request with "ChangeCipherSpec" and "Finished parameters by sending an EAP-Response/EAP-Type=EAP-TTLS with User-Name, MS-CHAP-Challenge, and MS-CHAP-Password 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	RFC 5281 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [2]: 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	RFC 5281 [12]. WFNA Stage3 [2]: 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	RFC 5281 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [2]: 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	RFC 5281 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [2]: 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-TTLS 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	RFC 5281 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [2]: 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 "ClientKeyExchange", "ChangeCipherSpec", and "Finished" parameters and then received an EAP-Request with "ChangeCipherSpec" and "Finished" parameters.
Expected Behaviour	Check that: The IUT in response to the EAP-Request message with ChangeCipherSpec" and "Finished" parameters sends an EAP-Response/EAP-Type=EAP-TTLS with User-Name, MS-CHAP-Challenge, and MS-CHAPPassword 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	RFC 5281 [12]. RFC 5246 [19]: section 7.3. WFNA Stage3 [2]: 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	RFC 5281 [12]: sections 9.1 and 9.2.2. WFNA Stage3 [2]: 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	RFC 5281 [12]: sections 9.1 and 9.2.2. WFNA Stage3 [2]: 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 [2]: 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 [2]: 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 [2]: 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 [1]: section 7.2.2. WFNA Stage3 [2]: section 4.11.4. RFC 4861 [14]. RFC 3315 [16]: section 5.3.
PICS Item	PIC_IP6
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 [1]: section 7.2.2. WFNA Stage3 [2]: section 4.11.4. RFC 4861 [14]. RFC 4862 [15].
PICS Item	PIC_IP6
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 [1]: section 7.2.2. WFNA Stage3 [2]: section 4.11.4. RFC 4861 [14]. RFC 4862 [15].
PICS Item	PIC_IP6
Initial Condition	IUT has completed authentication and the IUT is IPv6 capable.
Expected Behaviour	Check that: MS shall send 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 [2]: section 4.11.3. RFC 4861 [14]. RFC 4862 [15].
PICS Item	PIC_IP6
Initial Condition	IUT has completed set-up 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 [2]: section 4.11.3. RFC 4861 [14]. RFC 4862 [15].
PICS Item	PIC_IP6
Initial Condition	IUT has completed set-up 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	

TP ID	TP/MS/IPv6 /BV-H005
Reference	WFNA Stage2p2 [1]: section 7.2.2.3. WFNA Stage3 [2]: section 4.11.4.4. RFC 4861 [14]. RFC 4862 [15].
PICS Item	PIC_SAA
Initial Condition	IUT has completed set-up of IPv6 Initial Service Flow using stateful IP address assignment (DHCPv6)
Expected Behaviour	Check that: if when the lease lifetime for the assigned address is near to expire the IUT sends a RENEW message to extend the lifetime of the IP address.
Test strategy	
Notes	

TP ID	TP/MS/IPv6 /BV-H006
Reference	WFNA Stage3 [2]: sections 3.3.3 and 4.11.6. RFC 791 [5].
PICS Item	PIC_IP6
Initial Condition	IUT has completed set-up of IPv6 Initial Service Flow.
Expected Behaviour	Check that: when the IUT sends an UL IPv6 packet via the IPv6 Initial Service Flow exceeding the MTU size of 1400 bytes, the IPv6 packet is fragmented into more messages.
Test strategy	
Notes	Requires a means to make the IUT transmit an IPv6 packet exceeding the MTU size.

TP ID	TP/MS/IPv6 /BV-H007
Reference	WFNA Stage3 [2]: sections 3.3.3 and 4.11.6. RFC 791 [5].
PICS Item	PIC_IP6
Initial Condition	IUT has completed set-up of IPv6 Initial Service Flow.
Expected Behaviour	Check that: the IUT correctly receives IPv6 packets via the IPv6 Initial Service Flow which have been fragmented due to the size exceeding MTU size of 1400 bytes.
Test strategy	
Notes	

5.2.7   CMIPv6

TP ID	TP/MS/CMIPv6/BV-H000
Reference	WFNA Stage2p2 [1]: section 7.8.2.5.1. WFNA Stage3 [2]: section 4.8.4.1. RFC 3775 [17]: section 6.1.7. RFC 4285 [18], section 4.5.6.
PICS Item	PIC_CMIPv6.
Initial Condition	IUT has completed IPv6 Address assignment receiving the Home Address (HoA) using either stateful or stateless IP configuration. The IUT has not established an IPsec Security Association with the TE.
Expected Behaviour	Check that: The IUT sends a Binding Update message with the Destination Option Header and mobility header (MH type 5), and including the Mobile Message Authentication Option, the Mobile Node Identifier, and the received home address in the HoA field.
Test strategy	
Notes	

TP ID	TP/MS/CMIPv6/BV-H001
Reference	WFNA Stage2p2 [1]: section 7.8.2.5.3. WFNA Stage3 [2]: section 4.8.4.2. RFC 3775 [17]: section 6.1.7. RFC 4285 [18].
PICS Item	PIC_CMIPv6.
Initial Condition	IUT has completed IPv6 Address assignment but did not receive a Home Address (HoA) or HL prefix information in the DHCP Reply. The IUT has not established an IPsec Security Association with the TE.
Expected Behaviour	Check that: To register the IUT sends a Binding Update message with the HoA field set either to the unspecified address (0::0) or to a /64 Interface ID (IID).
Test strategy	
Notes	

TP ID	TP/MS/CMIPv6/BV-H002
Reference	WFNA Stage2p2 [1]: section 7.8.2.5.3. WFNA Stage3 [2]: 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	Note: If stateless IP address configuration is used to calculate the new CoA then DAD shall also be preformed.

TP ID	TP/MS/CMIPv6/BV-H003
Reference	WFNA Stage2p2 [1]: section 7.8.2.5.2. WFNA Stage3 [2]: 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-H004
Reference	WFNA Stage2p2 [1]: section 7.8.2.5.5. WFNA Stage3 [2]: 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 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-H005
Reference	WFNA Stage2p2 [1]: section 7.8.2.5.5. WFNA Stage3 [2]: 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-H006
Reference	[2] 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-H007
Reference	WFNA Stage3 [2]: 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 "Duplicate 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-H008
Reference	WFNA Stage2p2 [1]: section 7.8.2.14. WFNA Stage3 [2]: 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-H009
Reference	WFNA Stage2p2 [1]: section 7.8.2.14. WFNA Stage3 [2]: 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-H010
Reference	WFNA Stage2p2 [1]: section 7.8.2.14. WFNA Stage3 [2]: 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-H011
Reference	WFNA Stage2p2 [1]: section 7.8.2.14. WFNA Stage3 [2]: 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-H012
Reference	WFNA Stage2p2 [1]: section 7.8.2.14. WFNA Stage3 [2]: 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-H013
Reference	WFNA Stage2p2 [1]: section 7.8.2.14. WFNA Stage3 [2]: 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_Parameter_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 [1]: section 7.8.2.14. WFNA Stage3 [2]: 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_Parameter_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-H015
Reference	WFNA Stage2p2 [1]: section 7.8.2.14. WFNA Stage3 [2]: 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_Parameter_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-H016
Reference	WFNA Stage2p2 [1]: section 7.8.2.14. WFNA Stage3 [2]: 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_Parameter_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-H017
Reference	WFNA Stage2p2 [1]: section 7.8.2.14. WFNA Stage3 [2]: 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-H018
Reference	WFNA Stage3 [2]: 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	

5.2.7   Over-The-Air (OTA) Provisioning and Activation

TP ID	TP/MS/OTA/BV-H000
Reference	OTA-Gen [26]: section 9.2 WFNA Stage3 [2]: section 4.5.1 RFC 4282 [40]
PICS Item	PIC_OTA and (PIC_TPB1 or PIC_TPB2)
Initial Condition	The IUT is performing device authentication as part of network entry. Device is not activated
Expected Behaviour	Check that: The IUT sends an EAP-Response/Identity message in response to an EAP-Request/Identity message, the EAP/Response/Identity includes the WiMAX OTA provisioning service mode attribute value pair 'sm=1' as part of the NAI parameter.
Test strategy	
Notes	

TP ID	TP/MS/OTA/BV-H000a
Reference	OTA-Gen [26]: section 9.2 WFNA Stage3 [2]: section 4.5.1 RFC 4282 [40]
PICS Item	PIC_OTA and (PIC_TPB1 or PIC_TPB2)
Initial Condition	The IUT is performing device authentication as part of network entry. Device is activated
Expected Behaviour	Check that: The IUT sends an EAP-Response/Identity message in response to an EAP-Request/Identity message, the EAP/Response/Identity includes the NAI parameter without the WiMAX OTA provisioning service mode attribute value pair 'sm=1' as part of it.
Test strategy	
Notes	Setting Activate flag relying on TTCN code will be very difficult because of the need of performing NW-Entry, Service Flows establishment and OTA procedure through TTCN code. It would be necessary to find out another ways of reaching the initial condition for the test, in this case Activate flag set to true.

Common OMA and TR-069 protocol WIB procedures

TP ID	TP/MS/OTA/BV-H001
Reference	OTA-Gen [26]: sections 8 and 9.7 RFC 2782 [33]
PICS Item	PIC_OTA and PIC_WIB and (PIC_TPB1 or PIC_TPB2)
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT does not have access to the URL of the WIB server. Device is not activated
Expected Behaviour	Check that: The IUT sends a custom DNS query to the get URL of WIB server. The 'service' in the query is set to "wimax-bootstrap", the 'protocol' to "tcp". In addition to checking query/protocol and the set domain within the messaging.
Test strategy	
Notes	

TP ID	TP/MS/OTA/BV-H002
Reference	OTA-Gen [26]: section 9.7
PICS Item	PIC_OTA, PIC_WIB
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT does not have access to the URL of the WIB server.
Expected Behaviour	Check that: The IUT sends a DNS query to get URL of WIB server. The 'service' in the query is set to "wimax-bootstrap", the 'protocol' to "tcp" and the Name to the Domain Name obtained from DHCP procedure.
Test strategy	
Notes	SBC-RSP MUST not contain the target NSP realm.

TP ID	TP/MS/OTA/BV-H003
Reference	OTA-Gen [26]: section 9.2 WFNA Stage3 [2]: section 4.5.1 RFC 4282 [40]
PICS Item	PIC_OTA and (PIC_TPB1 or PIC_TPB2)
Initial Condition	The IUT is performing device authentication as part of network entry. Device is not activated
Expected Behaviour	Check that: When IUT is offered TLS for authentication, the IUT completes correctly authentication. IUT must use a decorated NAI for authentication.
Test strategy	
Notes	

TP ID	TP/MS/OTA/BV-H004
Reference	OTA-Gen [26]: section 9.2 WFNA Stage3 [2]: section 4.5.1 RFC 4282 [40]
PICS Item	PIC_OTA and (PIC_TPB1 or PIC_TPB2)
Initial Condition	The IUT is performing device authentication as part of network entry. Device is activated and EAP method is set to EAP-TTLS
Expected Behaviour	Check that: The IUT completes correctly authentication using EAP-TTLS method. IUT must use a non decorated NAI for authentication.
Test strategy	
Notes	Setting Activate flag relying on TTCN code will be very difficult because of the need of performing NW-Entry, Service Flows establishment and OTA procedure through TTCN code. It would be necessary to find out another ways of reaching the initial condition for the test, in this case Activate flag set to true.

TP ID	TP/MS/OTA/BV-H005
Reference	OTA-Gen [26]: section 9.2 WFNA Stage3 [2]: section 4.5.1 RFC 4282 [40]
PICS Item	PIC_OTA and (PIC_TPB1 or PIC_TPB2)
Initial Condition	The IUT is performing device authentication as part of network entry. A valid REALM record is available in the IUT.
Expected Behaviour	Check that: The IUT uses this REALM for authentication.
Test strategy	
Notes	Setting Activate flag relying on TTCN code will be very difficult because of the need of performing NW-Entry, Service Flows establishment and OTA procedure through TTCN code. It would be necessary to find out another ways of reaching the initial condition for the test, in this case a new value for REALM record.

5.2.7.1   OMA based

5.2.7.1.1   Bootstrap

Server Initiated Bootstrap

TP ID	TP/MS/OTA/OMA/BTS/BV-H000
Reference	OTA-OMA [28]: section 6.2.3.
PICS Item	PIC_OTA and PIC_OMA and PIC_SIB
Initial Condition	The IUT has completed pre-provisioning and has completed OMA server-initiated initial bootstrap procedure.
Expected Behaviour	Check that: when the IUT has successfully completed processing of the bootstrap document received in the UDP Push message, the IUT sends an OMA DM Package #1 to initiate a session with OMA DM server.
Problems	Not all devices will support this as some will block this messaging at the MS firewall. This will be optional
Test strategy	
Notes	

WIB procedure Bootstrap

TP ID	TP/MS/OTA/OMA/BTS/BV-H001
Reference	OTA-Gen [26]: sections 8 and 9.7. RFC-2616 [34]: section 9.3.
PICS Item	PIC_OTA and PIC_WIB and PIC_OMA
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT has performed successful WIB server location resolution.
Expected Behaviour	Check that: The IUT sends a HTTP GET message with Request-URI "/bootstrap.wib?version=VERSION&msid=MAC&protocol={ PROTOCOL}" where PROTOCOL contains the value '0' (OMA protocol).
Test strategy	
Notes	

TP ID	TP/MS/OTA/OMA/BTS/BV-H002
Reference	OTA-Gen [26]: sections 8, 9.7 and 9.7.1.
PICS Item	PIC_OTA and PIC_WIB and PIC_OMA
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT has performed successful WIB server location resolution and has sent the HTTP GET message.
Expected Behaviour	Check that: When the IUT receives a HTTP Response message containing duplicate TLVs, the IUT uses the first instance and ignores other ones.
Test strategy	
Notes	This can checked as the IUT continues to initiate OMA management session after the bootstrap procedure using the parameter value of the first TLV instances. In "WiMAX Forum OTA Provisioning System Specification, v.1.0.2" section 8, Figure 3 indicates the WIB procedure using HTTP and in section 9.7.1 (page 24 lines 9 and 10), it is stated: "If the bootstrap message contains duplicate TLVs'including the value fied, the first TLV SHALL be accepted and the other ones SHALL be ignored. The TP is therefore derived from the spec, what to do? We see two possibilities: a) Keep the TP, later decide what priority and whether it will be implemented or not Delete the TP even though that it may be correct as TP.

TP ID	TP/MS/OTA/OMA/BTS/BV-H003
Reference	OTA-Gen [26]: sections 8, 9.7 and 9.7.1.
PICS Item	PIC_OTA and PIC_WIB and PIC_OMA
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT has performed successful WIB server location and has sent the HTTP GET message.
Expected Behaviour	Check that: When the IUT receives a HTTP Response message containing invalid attributes the IUT does not continue the bootstrap procedure
Test strategy	
Notes	This can checked as the IUT does not initiate an OMA management session after the bootstrap procedure.

TP ID	TP/MS/OTA/OMA/BTS/BV-H004
Reference	OTA-Gen [26]: section 9.7.
PICS Item	PIC_OTA, PIC_WIB, PIC_OMA
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT has got the WIB server address from the DNS query exchange. IUT has sent a HTTP GET to the WIB server indicating the supported DM OTA protocols (OMA DM must be supported)
Expected Behaviour	Check that: When receiving an invalid bootstrap document, the IUT does not send OMA-DM PKG #1 but HTTP GET message in order to retry WIB procedure.
Test strategy	
Notes	Examples of invalid bootstrap document: no DM_ACC or BEK misalignment. WIB server must select OMA DM provisioning method.

5.2.7.1.2   Provisioning (OMA) Protocol

TP ID	TP/MS/OTA/OMA/PVS/BV-H000
Reference	OTA-OMA [28]: sections 6.5.1 and A.6. OMA-DMP [35] section 8.3.
PICS Item	PIC_OTA and PIC_OMA
Initial Condition	The IUT has completed pre-provisioning and has completed successful OMA server initiated initial bootstrap procedure.
Expected Behaviour	Check that: The IUT initiates OMA management session by sending a Package #1 message with the device information containing at least the Device manufacturer, Device Model, Device Client version, and Device Current Language setting information.
Test strategy	
Notes	WF Net.Arch. OTAProvisioning based on OMA DM spec says on page 16 lines 25-27: "Upon receiving the notification message, and - if necessary - confirmed by user interaction, the device 26 SHALL start an OMA DM session by sending an OMA DM Package #1 to the OMA DM server. Package 27 #1 SHALL contain DevInfo as describer in Annex A." Annex A (normative) defines DevInfo (fields that are required or optional).

Large objects

TP ID	TP/MS/OTA/OMA/PVS/BV-H001
Reference	OTA-OMA [28]: section 5.1.4. OMA-DMP [35]: sections 6.2 and 7.
PICS Item	PIC_OMA and PIC_LO
Initial Condition	The IUT has completed OMA bootstrap procedure and a management session is established.
Expected Behaviour	Check that: When the IUT is to send an object whose size exceeds that which can be transmitted in a single SyncML message, all SyncML messages sent to convey the object except the last one contain the element "<MoreData/>".
Test strategy	This tests OMA General Client Behavior and is not WiMAX Specific. Some level of OMA client behaviour must be tested.
Notes	Requires an object transfer causing splitting into more messages.

TP ID	TP/MS/OTA/OMA/PVS/BV-H002
Reference	OTA-OMA [28]: section 5.1.4. OMA-DMP [35]: sections 6.2 and 7.
PICS Item	PIC_OMA and PIC_LO
Initial Condition	The IUT has completed OMA bootstrap procedure and a management session is established.
Expected Behaviour	Check that: When the IUT is to send an object whose size exceeds that which can be transmitted in a single SyncML message, the SyncML message carrying the last part of the object contains the "Final" element.
Test strategy	This tests OMA General Client Behavior and is not WiMAX Specific. Some level of OMA client behaviour must be tested.
Notes	Requires an object transfer causing splitting into more messages.

TP ID	TP/MS/OTA/OMA/PVS/BV-H003
Reference	OTA-OMA [28]: section 5.1.4. OMA-DMP [35]: sections 6.2, 7 and 8.
PICS Item	PIC_OMA and PIC_LO
Initial Condition	The IUT has completed OMA bootstrap procedure and has sent package #1 (client initialization).
Expected Behaviour	Check that: When the IUT successfully receives a SyncML message containing a data object part and including the "<MoreData/>" element, the IUT responds with a status message "213 - Chunked item accepted and buffered"
Test strategy	This tests OMA General Client Behavior and is not WiMAX Specific. Some level of OMA client behaviour must be tested.
Notes	

TP ID	TP/MS/OTA/OMA/PVS/BV-H004
Reference	OTA-OMA [28]: section 5.1.4. OMA-DMP [35]: sections 6.2, 7 and 8.
PICS Item	PIC_OMA and PIC_LO
Initial Condition	The IUT has completed OMA bootstrap procedure and has sent package #1 (client initialization).
Expected Behaviour	Check that: When the IUT successfully receives a SyncML message containing the last part of a split data object including the "<Final/>" element, and the package from the server (TE) contains either a management operation or a challenge, the IUT includes the status of the reception of the object in the response message.
Test strategy	Not relevant for WiMAX. Do not need to test OMA-DM specific behaviour. Suggest not testing OMA-DM Client, but test only above OMA-DM (WiMAX specific) usage. II.e. a problem with OMA-DM client does not mean WIMAX will not function correctly - but this test does not check WiMAX flows Should not replace OMA-DM Client testing (external to WiMAX)
Notes	

TP ID	TP/MS/OTA/OMA/PVS/BV-H005
Reference	OTA-OMA [28]: section 5.1.4. OMA-DMP [35]: sections 6.2, 7 and 8.
PICS Item	PIC_OMA and PIC_LO
Initial Condition	The IUT has completed OMA bootstrap procedure and has sent package #1 (client initialization).
Expected Behaviour	Check that: When the IUT successfully receives a SyncML message containing the last part of a split data object including the "<Final/>" element, and the package from the server (TE) contains no a management operation or challenge, the IUT does not transmit any response message.
Test strategy	Not relevant for WiMAX. Do not need to test OMA-DM specific behaviour. Suggest not testing OMA-DM Client, but test only above OMA-DM (WiMAX specific) usage. II.e. a problem with OMA-DM client does not mean WIMAX will not function correctly - but this test does not check WiMAX flows Should not replace OMA-DM Client testing (external to WiMAX)
Notes	

TP ID	TP/MS/OTA/OMA/PVS/BV-H006
Reference	OTA-OMA [28]: section 6.5. OMA-DMP [35]: sections 6.2, 7, 8 and 9.
PICS Item	PIC_OMA and PIC_LO
Initial Condition	The IUT has completed OMA bootstrap procedure and has sent package #1 (client initialization) and received a Package #2 message from the server (TE) containing a challenge of the IUT.
Expected Behaviour	Check that: The IUT resends the Package #1 message (the same Alert and DevInfo parameters) and including the requested credentials.
Test strategy	Not relevant for WiMAX. Do not need to test OMA-DM specific behaviour. Suggest not testing OMA-DM Client, but test only above OMA-DM (WiMAX specific) usage. II.e. a problem with OMA-DM client does not mean WIMAX will not function correctly - but this test does not check WiMAX flows Should not replace OMA-DM Client testing (external to WiMAX)
Notes	

Continuous management (timer based session initiation)

TP ID	TP/MS/OTA/OMA/PVS/BV-H007
Reference	OTA-OMA [28]: sections 6.6, A9.6.9, A9.6.10 and A10.4.7.6. OMA-DMP [35]: section 8.2.
PICS Item	PIC_OMA and PIC_CM
Initial Condition	The IUT has completed OMA bootstrap procedure and indicated support for client initiated continuous management and with a value greater than zero for parameter " WiMAXSupp/Operator/<X>/NetworkParameters/PollingInterval" Condition is problematic: 1) this assumes it also completed first polling attempt after NE. The WiMAX...PollingInterval param: for this to be >0, the test equipment must provision this parameter. (requires additional messaging to bring client to this initial state) 2) If it makes sense to refer to the default value for WiMAX, then need to specify this here as well (alternate strategy to creating initial condition via the pre-WiMAX...PollingInterval messaging)
Expected Behaviour	Check that: The IUT sends a Package #1 message to initiate management session when the specified polling interval expires.
Test strategy	
Notes	

TP ID	TP/MS/OTA/OMA/PVS/BV-H008
Reference	OTA-Gen [26]: section 9.7.
PICS Item	PIC_OTA, PIC_WIB, PIC_OMA
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT has completed WIB procedure and the selected provisioning method is OMA DM. IUT has sent the OMA DM PKG #1 to the OMA DM server.
Expected Behaviour	Check that: when OMA DM server does not response to PKG #1, IUT retries WIB procedure by sending a new HTTP GET message.
Test strategy	
Notes	

TP ID	TP/MS/OTA/OMA/PVS/BV-H009
Reference	OTA-OMA-DM [28]: section A.10.4.7.6
PICS Item	PIC_OTA, PIC_WIB, PIC_OMA, PIC_POLLING_SUPPORT
Initial Condition	IUT has completed pre-provisioning phase, WIB procedure and the selected provisioning method is OMA DM. IUT has completed the OMA DM session in which OMA DM server has changed the value of Polling Interval in Wimax MO.
Expected Behaviour	Check that: IUT connects to the OMA DM server for polling-based client-initiated management session after the value indicated by the Polling Interval value.
Test strategy	
Notes	Polling Attempts must not be set to zero.

TP ID	TP/MS/OTA/OMA/PVS/BV-H010
Reference	
PICS Item	PIC_OTA, PIC_WIB, PIC_OMA
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT has completed WIB procedure and the selected provisioning method is OMA DM. IUT has sent the OMA DM PKG #1 to the OMA DM server.

Expected Behaviour	Check that: when OMA DM server sends OMA DM GET command to the OMA client querying with the following MO:
	
	• ./WiMAX/WiMAXRadioModule
	  o /<x>/Man/
	  o /<x>/Mod/
	  o /<x>/SwV/
	  o /<x>/HwV/
	  o /<x>/FwV/
	  o /<x>/MACAddress/
	  o /<x>/SPLock/LockStatus/
	  o /<x>/SPLock/Operator/
	  o /<x>/SPLock/VerNbr/
	  o /<x>/SPLock/Lock/
	• ./WiMAX/TerminalEquipment
	  o /DevType/
	  o /SwV/
	  o /HwV/
	  o /FwV/
	  o /DevID/
	  o /Man/
	  o /Mod/
	• ./WiMAX/TO-WiMAX-REF/
	• ./WiMAX/DevCap/IPCap
	  o /IPv4/
	  o /IPv6/
	  o /CMIPv4/
	  o /CMIPv6/
	• ./WiMAX/DevCap/UpdateMethods
	  o /ServerInitiated/
	  o /ClientInitiated/PollingSupported/
	/ClientInitiated/PollingInterval/
	
	IUT will reply with the correct information.

Test strategy	
Notes	

TP ID	TP/MS/OTA/OMA/PVS/BV-H011
Reference	
PICS Item	PIC_OTA, PIC_WIB, PIC_OMA
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT has completed WIB procedure and the selected provisioning method is OMA DM. IUT has sent the OMA DM PKG #1 to the OMA DM server.

Expected Behaviour	Check that: when OMA DM server sends OMA DM REPLACE command to the OMA client for replacing the following MO:
	
	• ./WiMAX/WiMAXRadioModule
	  o /<x>/Man/
	  o /<x>/Mod/
	  o /<x>/SwV/
	  o /<x>/HwV/
	  o /<x>/FwV/
	  o /<x>/MACAddress/
	  o /<x>/SPLock/LockStatus/
	  o /<x>/SPLock/Operator/
	  o /<x>/SPLock/VerNbr/
	  o /<x>/SPLock/Lock/
	• ./WiMAX/TerminalEquipment
	  o /DevType/
	  o /SwV/
	  o /HwV/
	  o /FwV/
	  o /DevID/
	  o /Man/
	  o /Mod/
	• ./WiMAX/TO-WiMAX-REF/
	• ./WiMAX/DevCap/IPCap
	  o /IPv4/
	  o /IPv6/
	  o /CMIPv4/
	  o /CMIPv6/
	• ./WiMAX/DevCap/UpdateMethods
	  o /ServerInitiated/
	  o /ClientInitiated/PollingSupported/
	/ClientInitiated/PollingInterval/
	
	IUT will refuse the change by a query showing that parameters were not changed.

Test strategy	
Notes	

TP ID	TP/MS/OTA/OMA/PVS/BV-H012
Reference	
PICS Item	PIC_OTA, PIC_WIB, PIC_OMA
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT has completed WIB procedure and the selected provisioning method is OMA DM. IUT has sent the OMA DM PKG #1 to the OMA DM server.

Expected Behaviour	Check that: when OMA DM server sends OMA DM ADD command to the OMA client in order to populate the following leafs of Wimax MO:
	
	• ./WiMAXSupp/Operator/<x>/NetworkParameters
	  o /H-NSP/<x>/H-NSP-ID/
	  o /CAPL/Entries/<x>/NAP-ID/
	  o CAPL/Entries/<x>/Priority/
	  o /CAPL/Entries/<x>/ChPlanRefIds/<x>/RefId/
	  o /CAPL/SelectPolicy/
	  o /RAPL/Entries/<x>/V-NSP-ID/
	  o /RAPL/Entries/<x>/Priority/
	  o /RAPL/SelectPolicy/
	  o /ChannelPlan/Entries/<x>/Id/
	  o /ChannelPlan/Entries/<x>/FirstFreq/
	  o /ChannelPlan/Entries/<x>/LastFreq/
	  o /ChannelPlan/Entries/<x>/NextFreqStep/
	  o /ChannelPlan/Entries/<x>/Preambles/
	  o /ChannelPlan/Entries/<x>/BW/
	  o /ChannelPlan/Entries/<x>/FFTSize/
	  o /ChannelPlan/Entries/<x>/DuplexMode/
	  o /ChannelPlan/BW/
	  o /ChannelPlan/FFTSize/
	  o /ChannelPlan/DuplexMode/
	  o /OperatorName/
	  o /PollingInterval/
	• ./WiMAXSupp/Operator/<x>/SubscriptionParameters
	  o /Primary/EAP/<x>/METHOD-TYPE/
	  o /Primary/EAP/<x>/VENDOR-ID/
	  o /Primary/EAP/<x>/VENDOR-TYPE/
	  o /Primary/EAP/<x>/USER-IDENTITY/
	  o /Primary/EAP/<x>/PROVISIONED-PSEUDO-IDENTITY/
	  o /Primary/EAP/<x>/PASSWORD/
	  o /Primary/EAP/<x>/REALM/
	  o /Primary/EAP/<x>/USE-PRIVACY/
	  o /Primary/EAP/<x>/ENCAPS/
	  o /Primary/EAP/<x>/CERT/<x>/CERT-TYPE/
	  o /Primary/EAP/<x>/CERT/1/CERT-TYPE/
	  o /Primary/EAP/<x>/VFY-SERVER-REALM/
	  o /Primary/Name/
	  o /Primary/Activated/
	./WiMAXSupp/Operator/<x>/To-IP-REF/
	
	After querying for these parameters, the IUT will supply the provisioned information.

Test strategy	
Notes	

5.2.7.2 TR-069 based

These tests will be performed for MS indicating support for OTA TR-069 based provisioning and activation.

5.2.7.2.1   Bootstrap

TP ID	TP/MS/OTA/T69/BTS/BV-H000
Reference	OTA-Gen [26] sections 8 and 9.7. RFC-2616 [34] section 9.3.
PICS Item	PIC_OTA and PIC_WIB and PIC_TR069
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT has performed successful WIB server location.
Expected Behaviour	Check that: The IUT sends a HTTP GET message with Request-URI ""/bootstrap.wib?version=VERSION&msid=MAC&protocol={ PROTOCOL}" where PROTOCOL contains the value '1' (TR-069 protocol).
Test strategy	
Notes	

TP ID	TP/MS/OTA/T69/BTS/BV-H001
Reference	OTA-Gen [26]: sections 8, 9.7 and 9.7.1. RFC-2616 [34]: section 6.
PICS Item	PIC_OTA and PIC_WIB and PIC_TR069
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT has performed successful WIB server location and has sent the HTTP GET message.
Expected Behaviour	Check that: When the IUT receives a HTTP Response message containing duplicate TLVs, the IUT uses the first instance and ignores other ones.
Test strategy	
Notes	This can checked as the IUT after successful bootstrap procedure will send Inform request message to initiate a session with the ACS (Auto-Configuration Server).

TP ID	TP/MS/OTA/T69/BTS/BV-H002
Reference	OTA-Gen [26]: sections 8, 9.7 and 9.7.1. RFC-2616 [34]: section 6.
PICS Item	PIC_OTA and PIC_WIB and PIC_TR069
Initial Condition	IUT has completed pre-provisioning phase and is to perform OTA initial bootstrap procedure using WIB. The IUT has performed successful WIB server location and has sent the HTTP GET message.
Expected Behaviour	Check that: When the IUT receives a HTTP Response message containing invalid attributes the IUT does not continue the bootstrap procedure
Test strategy	
Notes	This can checked as the IUT does not initiate a session with the ACS (Auto-Configuration Server) after the bootstrap procedure ends.

5.2.7.2.2   Provisioning

TP ID	TP/MS/OTA/T69/PVS/BV-H000
Reference	OTA-TR069 [27]: section 5.4. OTA-Gen [26]: sections 7.1, 8 and 9.7. DSL-TR069 [36]: section 3.7.
PICS Item	PIC_OTA and PIC_TR069 and PIC_B1
Initial Condition	IUT has completed pre-provisioning phase and has successfully completed OTA initial bootstrap procedure using WIB, i.e. the IUT has received all necessary bootstrap parameters from the WIB server in the HTTP response message
Expected Behaviour	Check that: The IUT sends an initial Inform request message to the ACS (Auto-Configuration Server) in an HTTP POST message
Test strategy	
Notes	

TP ID	TP/MS/OTA/T69/PVS/BV-H001
Reference	OTA-TR069 [27]: section 5.2. DSL-TR069 [36]: sections 3.7 and 3.2.1, Table 3.
PICS Item	PIC_OTA and PIC_TR069 and PIC_B1
Initial Condition	IUT has completed pre-provisioning phase and has successfully completed OTA initial bootstrap procedure using WIB, i.e. the IUT has received all necessary bootstrap parameters from the WIB server in the HTTP response message. The IUT has sent an Inform request message to initiate a connection to the ACS.
Expected Behaviour	Check that: when the IUT does not receive an InformResponse message, the IUT resends the Inform Request message according to the Wait interval range specified in Table 3.
Test strategy	
Notes	

5.2.8   Emergency Services

TP ID	TP/MS/EMG/BV-H000
Reference	[29]: section 7.2.
PICS Item	PIC_EMG_VOIP and PIC_EMG_RCG
Initial Condition	IUT is not attached to any network
Expected Behaviour	Check that: When the IUT initiates an Emergency Service call during the EAP Authentication Procedure, the IUT sets the outer NAI to {sm=2} <username>@<NSPRealm>
Test strategy	
Notes	

TP ID	TP/MS/EMG/BV-H001
Reference	[29]: section 7.1.1.1.
PICS Item	PIC_EMG_VOIP and PIC_EMG_RCG
Initial Condition	The IUT has performed Emergency Service access
Expected Behaviour	Check that: When the IUT terminates and performs normal access the MS does not use the emergency decoration when re-entering the network
Test strategy	
Notes	

TP ID	TP/MS/EMG/BV-H002
Reference	[29]: section 9.2. [37]: sections 1 and 3.
PICS Item	PIC_EMG_SIP and PIC_EMG_VOIP
Initial Condition	The IUT has performed Emergency Service access
Expected Behaviour	Check that: The IUT sets the special indication in the outgoing SIP messages according to the type of emergency call "urn:service:sos".
Test strategy	
Notes	

5.2.9   Location Based Services

TP ID	TP/MS/LBS/BV-H000
Reference	[31]: annex D.
PICS Item	PIC_LBS
Initial Condition	The IUT has performed network entry and did not include Location Server Address request in the DHCP Request message during IP address acquisition.
Expected Behaviour	Check that: The IUT sends a DHCP Inform message with a DHCP Option to obtain the Location Server address.
Test strategy	
Notes	Require that the IUT can be controlled not to include the Location Server request in the initial IP address acquisition.

TP ID	TP/MS/LBS/BV-H001
Reference	[31]: annex D.
PICS Item	PIC_LBS
Initial Condition	The IUT has performed network entry and included Location Server Address request in the DHCP Request message for IP address acquisition and received the Location Server address in the DHCP Ack message.
Expected Behaviour	Check that: The IUT does not send a DHCP Inform message with a DHCP Option to obtain Location Server address(es).
Test strategy	
Notes	Require that the IUT can be controlled to include the Location Server request in the initial IP address acquisition.

TP ID	TP/MS/LBS/BV-H002
Reference	[31]: sections 9.5.1.4 and 8.3.4.
PICS Item	PIC_LBS and PIC_WLPN
Initial Condition	The IUT has performed network entry
Expected Behaviour	Check that: When the IUT establishes connection to the Location Server it sends a message indicating the Location Services capabilities it supports.
Test strategy	
Notes	Require that the IUT can be controlled to perform Capability negotiation.

TP ID	TP/MS/LBS/BV-H003
Reference	[31]: section 8.3.3.1.2.2.
PICS Item	PIC_LBS and PIC_AGPS
Initial Condition	The IUT has performed network entry and the TE has sent an AGPS-RSP message to cause the IUT to measure or calculate the location
Expected Behaviour	Check that: The IUT sends back a response message containing the measured location or the measured parameters if the IUT cannot calculate the location.
Test strategy	
Notes	

TP ID	TP/MS/LBS/BV-H004
Reference	[31]: sections 9.5.2.1 and 8.3.4. [35]: section 5.1.1.
PICS Item	PIC_LBS and PIC_SUPL
Initial Condition	The IUT has performed network entry and received a valid SUPL INIT message from the TE indicating that proxy mode is used.
Expected Behaviour	Check that: The IUT responds with a SUPL POS INIT message containing at least Session ID and IUT supported positioning methods.
Test strategy	
Notes	

TP ID	TP/MS/LBS/BV-H005
Reference	[31]: sections 9.5.2.1 and 8.3.4. [35]: section 5.1.1.
PICS Item	PIC_LBS and PIC_SUPL
Initial Condition	The IUT has performed network entry and received a non authentic SUPL INIT message from the TE
Expected Behaviour	Check that: The IUT discards the received message and do not send a response.
Test strategy	
Notes	

5.2.10   IP-IMS Interworking

TP ID	TP/MS/IMS/BV-H000
Reference	[30]: section 7.2.
PICS Item	PIC_IMS and (PIC_CMIPv4 or CMIPv6)
Initial Condition	The IUT has performed network entry and CMIP Registration.
Expected Behaviour	Check that: The |UT sends DHCP Inform message to acquire P-CSCF or a list of FQDN addresses.
Test strategy	
Notes	

TP ID	TP/MS/IMS/BV-H001
Reference	[30]: sections 7.2 and 8.3.1.
PICS Item	PIC_IMS and (PIC_CMIPv4 or CMIPv6)
Initial Condition	The IUT has performed network entry and CMIP Registration. The IUT has sent a DHCP Inform message and received a list of FQDN addresses
Expected Behaviour	Check that: The |UT performs a DNS query to retrieve a list of P-CSCF IP addresses.
Test strategy	
Notes	

TP ID	TP/MS/IMS/BV-H002
Reference	[30]: section 8.2 and 8.2.1. [39]: section 5.1.1.2.
PICS Item	PIC_IMS
Initial Condition	The IUT has perform initial network entry and CMIP registration and discovered a P-CSCF
Expected Behaviour	Check that: The IUT sends a SIP REGISTRATION request containing a private SIP header with P-Access-Network Info value "P-Access-Network-Info: WMF-Mobile WiMAX; wimax-bs-id=nnnnnnssssss where nnnnnn is a 3 octet string for the NAP operator ID and ssssss a 3 octet string for the base station ID
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
V1.2.1	November 2009	Publication