Enabler Test Specification for Client Provisioning v1.1

Candidate Version 1.1 – 21 Apr 2008

Open Mobile Alliance

OMA-ETS-Client Provisioning-V1_1-20080421-C

Use of this document is subject to all of the terms and conditions of the Use Agreement located at
http://www.openmobilealliance.org/UseAgreement.html.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the "OMA IPR Declarations" list at http://www.openmobilealliance.org/ipr.html. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE "OMA IPR DECLARATIONS" LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

1. Scope

This document describes in detail available test cases for Client Provisioning Enabler Release 1.1, http://www.openmobilealliance.org/ .

The test cases are split in two categories, conformance and interoperability test cases.

The conformance test cases are to verify the adherence to normative requirements described in the technical specifications.

The interoperability test cases are to verify that implementations of the specifications work satisfactory.

If either conformance or interoperability tests do not exists at the creation of the test specification this part should be marked not available.

2. References

2.1 Normative References

[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997. http://www.ietf.org/rfc/rfc2119.txt
[E2ESEC]	"Transport Layer End to End Security Specification", WAP Forum™, WAP-187-E2ESEC, http://www.openmobilealliance.org/
[PROVBOOT]	"Provisioning Bootstrap 1.1". Open Mobile Alliance™. OMA-WAP-ProvBoot-v1_1, http://www.openmobilealliance.org/
[PROVCONT]	"Provisioning Content 1.1", Open Mobile Alliance™, OMA-WAP-ProvCont-v1_1, http://www.openmobilealliance.org/
[PROVSC]	"Provisioning Smart Card 1.1", Open Mobile Alliance™, OMA-WAP-ProvSC-v1_1, http://www.openmobilealliance.org/
[PROVUAB]	"Provisioning User Agent Behaviour 1.1", Open Mobile Alliance™, OMA-WAP-ProvUABv1_1, http://www.openmobilealliance.org/
[WAPARCH]	"WAP Architecture". WAP Forum™. WAP-210-WAPArch, http://www.openmobilealliance.org/
[WAPPUSH]	"Push Architectural Overview", WAP Forum™, WAP-250-PushArchitecture, http://www.openmobilealliance.org/

2.2 Informative References

[OMADICT]	"Dictionary for OMA specifications". Open Mobile Alliance™. OMA-Dictionary-v2_6. http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1   Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except "Scope" and "Introduction", are normative, unless they are explicitly indicated to be informative.

The following numbering scheme is used:

xxx-y.z-con-number where:

xxx	Name of enabler, e.g. MMS or Browsing
y.z	Version of enabler release, e.g. 1.2 or 1.2.1
con	Indicating this test is a conformance test case
number	Leap number for the test case

Or

xxx-y.z-int-number where:

xxx	Name of enabler, e.g. MMS or Browsing
y.z	Version of enabler release, e.g. 1.2 or 1.2.1
int	Indicating this test is a interoperability test case
number	Leap number for the test case

3.2   Definitions

Application Access Information
Information provisioned into the phone that relate to identity and applications rather than to plain connectivity.
Bootstrap Document
A connectivity or application access document with information of relevance to the bootstrap process only.
Bootstrap process (bootstrapping)
The process by which the unconfigured ME is taken from the initial state to or through the TPS Access State. This process can be system specific.
Bootstrap Server
Bootstrap Server is the sender of the bootstrap message. It may physically be co-located with a TPS but that is irrelevant from an architecture point of view. The address of the Bootstrap Server is not relevant.
Configuration Context
A Configuration Context is a set of connectivity and application configurations typically associated with a single TPS. However, the Configuration Context can also be independent of any TPS. A TPS can be associated with several Configuration Contexts, but a TPS cannot provision a device outside the scope of the Configuration Contexts associated with that particular TPS. In fact, all transactions related to provisioning are restricted to the Configuration Contexts associated with the TPS.
Connectivity Information
This connectivity information relates to the parameters and means needed to access WAP infrastructure. This includes network bearers, protocols, access point addresses as well as proxy, DNS, and application access addresses and Trusted Provisioning Server URLs.
Continuous provisioning
The process by which the ME is provisioned with further infrastructure information at or after the TPS Access state. The information received during the bootstrap may be modified. This process is generic and optional. Continuous implies that the process can be repeated multiple times, but not that it is an ongoing activity.
Logical Proxy
A logical proxy is a set of physical proxies that may share the same WSP and WTLS context (shared session id value space). This implies that physical proxies within a logical proxy share the same WSP and WTLS session cache. For example, the device does not have to create a new WTLS session when switching

from CSD to SMS if the target is the same logical proxy.

MMS Proxy-Relay

A server that provides access to various messaging systems. It may operate as a WAP origin server in which case it may be able to utilize features of the WAP system.

Network Access Point

A physical access point is an interface point between the wireless network and the fixed network. It is often a Remote Access Server, an SMSC, a USSDC, or something similar. It has an address (often a telephone number) and an access bearer.

Origin Server

The server on which a given resource resides or is to be created. Often referred to as a web server or an HTTP server.

Physical Proxy

A physical proxy is a specific address with proxy functionality. It can be the IP address plus port for an IP accessible proxy, or the SME-address plus port for an SMS accessible proxy.

Privileged Configuration Context

A privileged configuration context is a special context in which it is possible to define the number of additional configuration contexts allowed. Not all WAP service providers are, however, allowed to bootstrap the privileged context.

Provisioned state

The state in which the ME has obtained connectivity information extending its access capabilities for content, applications or continuous provisioning. This state is reached when the bootstrap process has provided access to generic proxies, or the continuous provisioning process has been performed.

Provisioning document

A particular instance of an XML document encoded according to the provisioning content specification [PROVCONT].

Proxy Navigation

An in-band mechanism to provision the device in real time as defined in [E2ESEC].

Push Proxy

A WAP Push Proxy is a gateway intended to provide push connectivity between wired and wireless networks.

Trusted Provisioning Server

A Trusted Provisioning Server, is a source of provisioning information that can be trusted by a Configuration Context. They are the only entities that are allowed to provision the device with static configurations. In some cases, however, a single TPS is the only server allowed to configure the phone. Provisioning related to a specific TPS is restricted to Configuration Contexts that are associated with this TPS.

Trusted Provisioning Server Access State

The state in which the ME has obtained a minimum set of infrastructure components that enable the ME to establish the first communication channel(s) to WAP infrastructure, i.e. a trusted WAP proxy. This allows continuous provisioning, but may also provide sufficient information to the ME to access any other WAP content or application.

Trusted Proxy

The trusted (provisioning) proxy has a special position as it acts as a front-end to a trusted provisioning server. The trusted proxy is responsible to protect the end user from malicious configuration information.

3.3   Abbreviations

DNS	Domain Name System
IP	Internet Protocol
ME	Mobile Equipment
MMS	Multimedia Messaging Service
MSC	Mobile Switching Centre
NAP	Network Access Point
OTA	Over The Air

PX	Proxy
SIM	Subscriber Identification Module
SIM ATK	SIM Application Toolkit
SMSC	Short Message Service Centre
TPS	Trusted Provisioning Server
URL	Uniform Resource Locator
USSDC	Unstructured Supplementary Service Data Centre
WAP	Wireless Application Protocol
WIM	WAP Identification Module
WSP	WAP Session Protocol
WTA	Wireless Telephony Application
WTLS	Wireless Transport Layer Security
WWW	World Wide Web

4. Introduction

The purpose of this document is to provide test cases for Client Provisioning Enabler Release 1.1.

Some features in the Client Provisioning enabler may optionally be implemented in mobile devices. If an implementation states in their ICS that an optional feature is supported, then the tests for the optional feature are mandatory for that implementation. All the features that are supported will be tested if possible.

The following items on an overall level are needed to adequately test the Client Provisioning enabler:

- A Client Provisioning client to be configured.

- A Client Provisioning Server aka Trusted Provisioning Server (TPS) connected to the Internet

- A Smart Card with provisioning content

For the purpose of the test cases, the following Reference XML Configuration Messages have been created:

- UAB.xml

- Client_provisioning_doc_1.xml

- Client_provisioning_doc_2.xml

- Bootstrap_zero.xml

These Reference Configuration Messages are included in the Appendix B of this document and are referenced from each applicable test case. These XML documents shall be WBXML encoded in the Server / Smart Card

5. Client Provisioning Conformance Test Cases

5.1 User Agent Behaviour

The purpose of these tests are to verify that the Client Provisioning client is compliant to the Client Provisioning specification when receiving a provisioning document that is syntactically correct but semantically erroneous. (User Agent Behaviour reference configuration message can be found in Appendix B of this document.)

5.1.1 Redundant Characteristic ignored

Test Case Id	ClientProvisioning-1.1-con-001
Test Object	Client device
Test Case Description	The purpose of this test is to verify that if in the provisioning document a characteristic is redefined, the original definition prevails and the client ignores the second definition of the characteristic.
Specification Reference	[PROVUAB] Chapter 4.1
SCR Reference	ProvUAB-UCR-C-001
Preconditions	▪ A Client Provisioning client to be configured. ▪ A Client Provisioning server connected to the Internet. ▪ A Client Provisioning server with provisioning document UAB.xml
Test Procedure	1. In the server, send provisioning document UAB.xml to the client 2. The client receives the provisioning document UAB.xml 3. Verify the pass criteria below
Pass-Criteria	1. The client is able to receive the provisioning document UAB.xml correctly. 2. The client is able to save the received document. 3. The client is able to understand the provisioning document received. 4. The original definition of the redundant characteristic prevails.

5.1.2 Redundant Parameter ignored

Test Case Id	ClientProvisioning-1.1-con-002
Test Object	Client device
Test Case Description	The purpose of this test is to verify that if in the provisioning document a parameter is redefined, the original definition prevails and the client ignores the second definition of the parameter.
Specification Reference	[PROVUAB] Chapter 4.1
SCR Reference	ProvUAB-UCR-C-002
Preconditions	▪ A Client Provisioning client to be configured. ▪ A Client Provisioning server connected to the Internet. ▪ A Client Provisioning server with provisioning document UAB.xml
Test Procedure	1. In the server, send provisioning document UAB.xml to the client

	2. The client receives the provisioning document UAB.xml
	3. Verify the pass criteria below
Pass-Criteria	1. The client is able to receive the provisioning document UAB.xml correctly.
	2. The client is able to save the received document.
	3. The client is able to understand the provisioning document received.
	4. The original definition of the redundant parameter prevails.

5.1.3   Unknown characteristic ignored

Test Case Id	ClientProvisioning-1.1-con-003
Test Object	Client device
Test Case Description	The purpose of this test is to verify that if in the provisioning document an unknown characteristic is defined, the Client Provisioning client is able to ignore the unknown characteristic(s)
Specification Reference	[PROVUAB] Chapter 4.1
SCR Reference	ProvUAB-UCR-C-003
Preconditions	▪ A Client Provisioning client to be configured.
	▪ A Client Provisioning server connected to the Internet.
	▪ A Client Provisioning server with provisioning document UAB.xml
Test Procedure	1. In the server, send provisioning document UAB.xml to the client
	2. The client receives the provisioning document UAB.xml
	3. Verify the pass criteria below
Pass-Criteria	1. The client is able to receive the provisioning document UAB.xml correctly.
	2. The client is able to save the received document.
	3. The client is able to understand the provisioning document received.
	4. The unknown characteristic(s) is ignored.

5.1.4   Unknown parameter ignored

Test Case Id	ClientProvisioning-1.1-con-004
Test Object	Client device
Test Case Description	The purpose of this test is to verify that if in the provisioning document an unknown parameter is defined, the Client Provisioning client is able to ignore the unknown parameter(s)
Specification Reference	[PROVUAB] Chapter 4.1
SCR Reference	ProvUAB-UCR-C-004
Preconditions	▪ A Client Provisioning client to be configured.
	▪ A Client Provisioning server connected to the Internet.
	▪ A Client Provisioning server with provisioning document UAB.xml

Test Procedure	1. In the server, send provisioning document UAB.xml to the client
	2. The client receives the provisioning document UAB.xml
	3. Verify the pass criteria below
Pass-Criteria	1. The client is able to receive the provisioning document UAB.xml correctly.
	2. The client is able to save the received document.
	3. The client is able to understand the provisioning document received.
	4. The unknown parameter(s) is ignored.

5.1.5 Unknown value ignored

Test Case Id	ClientProvisioning-1.1-con-005
Test Object	Client device
Test Case Description	The purpose of this test is to verify that if in the provisioning document an unknown value for a parameter is defined, the Client Provisioning client is able to ignore the parameter(s) with unknown value(s)
Specification Reference	[PROVUAB] Chapter 4.1
SCR Reference	ProvUAB-UCR-C-005
Preconditions	▪ A Client Provisioning client to be configured.
	▪ A Client Provisioning server connected to the Internet.
	▪ A Client Provisioning server with provisioning document UAB.xml
Test Procedure	1. In the server, send provisioning document UAB.xml to the client
	2. The client receives the provisioning document UAB.xml
	3. Verify the pass criteria below
Pass-Criteria	1. The client is able to receive the provisioning document UAB.xml correctly.
	2. The client is able to save the received document.
	3. The client is able to understand the provisioning document received.
	4. The parameter(s) with the unknown value is ignored.

5.1.6 Physical proxy defined multiple times

Test Case Id	ClientProvisioning-1.1-con-006
Test Object	Client device
Test Case Description	The purpose of this test is to verify that if in the provisioning document a physical proxy is defined multiple times, the latter definition has lower priority and the conflict resolution rules defined for interdocument interaction are applied (section 5.2 in OMA-WAP-ProvUAB-v1_1-200211113-C)
Specification Reference	[PROVUAB] Chapter 4.1
SCR Reference	ProvUAB-U-C-005

Preconditions	▪ A Client Provisioning client to be configured.
	▪ A Client Provisioning server connected to the Internet.
	▪ A Client Provisioning server with provisioning document UAB.xml
Test Procedure	1. In the server, send provisioning document UAB.xml to the client
	2. The client receives the provisioning document UAB.xml
	3. Verify the pass criteria below
Pass-Criteria	1. The client is able to receive the provisioning document UAB.xml correctly.
	2. The client is able to save the received document.
	3. The client is able to understand the provisioning document received.
	4. The physical proxy defined multiple times is set to the first value defined in the provisioning document and the latter definition(s) of redundant parameters are discarded and the new parameters defined are added

5.1.7 Logical proxy defined multiple times

Test Case Id	ClientProvisioning-1.1-con-007
Test Object	Client device
Test Case Description	The purpose of this test is to verify that if in the provisioning document a logical proxy is defined multiple times, the latter definition has lower priority and the conflict resolution rules defined for interdocument interaction are applied (section 5.2 in OMA-WAP-ProvUAB-v1_1-200211113-C)
Specification Reference	[PROVUAB] Chapter 4.1
SCR Reference	ProvUAB-U-C-005
Preconditions	▪ A Client Provisioning client to be configured.
	▪ A Client Provisioning server connected to the Internet.
	▪ A Client Provisioning server with provisioning document UAB.xml
Test Procedure	1. In the server, send provisioning document UAB.xml to the client
	2. The client receives the provisioning document UAB.xml
	3. Verify the pass criteria below
Pass-Criteria	1. The client is able to receive the provisioning document UAB.xml correctly.
	2. The client is able to save the received document.
	3. The client is able to understand the provisioning document received.
	4. The logical proxy defined multiple times is set to the first value defined in the provisioning document and the latter definition(s) of redundant parameters are discarded and the new parameters defined are added

5.1.8 Redundant NAP definitions discarded

Test Case Id	ClientProvisioning-1.1-con-008
Test Object	Client device

Test Case Description	The purpose of this test is to verify that if in the provisioning document a NAP is defined multiple times, the latter definition is discarded
Specification Reference	[PROVUAB] Chapter 4.1
SCR Reference	ProvUAB-UCR-C-006
Preconditions	▪ A Client Provisioning client to be configured. ▪ A Client Provisioning server connected to the Internet. ▪ A Client Provisioning server with provisioning document UAB.xml
Test Procedure	1. In the server, send provisioning document UAB.xml to the client 2. The client receives the provisioning document UAB.xml 3. Verify the pass criteria below
Pass-Criteria	1. The client is able to receive the provisioning document UAB.xml correctly. 2. The client is able to save the received document. 3. The client is able to understand the provisioning document received. 4. The physical proxy defined multiple times is set to the first value defined in the provisioning document and the latter definition(s) are discarded

5.1.9 NAP defined for not supported bearer

Test Case Id	ClientProvisioning-1.1-con-009
Test Object	Client device
Test Case Description	The purpose of this test is to verify that if in the provisioning document a NAP is defined for a bearer that is not supported, this is ignored
Specification Reference	[PROVUAB] Chapter 4.2
SCR Reference	ProvUAB-UDP-C-001
Preconditions	▪ A Client Provisioning client to be configured. ▪ A Client Provisioning server connected to the Internet. ▪ A Client Provisioning server with provisioning document UAB.xml
Test Procedure	1. In the server, send provisioning document UAB.xml to the client 2. The client receives the provisioning document UAB.xml 3. Verify the pass criteria below
Pass-Criteria	1. The client is able to receive the provisioning document UAB.xml correctly. 2. The client is able to save the received document. 3. The client is able to understand the provisioning document received. 4. The NAP defined for the bearer(s) that is not supported is ignored

5.1.10 Physical proxy defined without a valid NAP

Test Case Id	ClientProvisioning-1.1-con-010

Test Object	Client device
Test Case Description	The purpose of this test is to verify that if in the provisioning document a physical proxy is defined without a valid NAP, this is ignored
Specification Reference	[PROVUAB] Chapter 4.2
SCR Reference	ProvUAB-UDP-C-003
Preconditions	▪ A Client Provisioning client to be configured. ▪ A Client Provisioning server connected to the Internet. ▪ A Client Provisioning server with provisioning document UAB.xml
Test Procedure	1. In the server, send provisioning document UAB.xml to the client 2. The client receives the provisioning document UAB.xml 3. Verify the pass criteria below
Pass-Criteria	1. The client is able to receive the provisioning document UAB.xml correctly. 2. The client is able to save the received document. 3. The client is able to understand the provisioning document received. 4. The physical proxy defined without a valid NAP is ignored

6. Client Provisioning Interoperability Test Cases

The reference configuration messages as applicable for Client Provisioning Interoperability test cases can be found in Appendix B of this document.

6.1 Bootstrap – Initial connectivity information, OTA

6.1.1 Using NETWPIN Authentication Mechanism

Test Case Id	ClientProvisioning-1.1-int-001a
Test Object	Client and Server device
Test Case Description	Purpose of this verification is to ensure that a server and a client are able to communicate the mandatory initial connectivity information: basic transport connectivity information that includes parameters for network access points and the proxies that are to be used. NETWPIN authentication mechanism shall be used.
Specification Reference	[PROVBOOT] Chapters 4.1 and 5 [PROVUAB] Chapters 4.1 and 4.2 [PROVCONT] Chapters 4.6.8 and 4.6.15
SCR Reference	ProvBoot-B-C-008 ProvBoot-B-C-011 ProvUAB-UDP-C-001 ProvUAB-UDP-C-002 ProvUAB-UDP-C-003 ProvUAB-UDP-C-006 ProvUAB-UDP-C-010 ProvUAB-UDP-C-011 ProvUAB-UDP-C-012 ProvUAB-UDP-C-013 ProvUAB-UDP-C-014 ProvUAB-UDP-C-015 ProvUAB-UEH-C-002 ProvCont-CC-C-001 ProvCont-CC-C-002 ProvCont-CC-C-004 ProvCont-CC-C-006 ProvCont-CC-C-015 ProvCont-CC-C-001 ProvBoot-BSF-C-001
Preconditions	▪ A Client Provisioning client to be configured. The client must have at least one network bearer. ▪ A Client Provisioning server connected to the internet. ▪ The receiving end doesn't have existing bootstrap context i.e. client is in unconfigured state.
Test Procedure	1. Create a configuration context on the provisioning server including the parameters for NETWPIN security mechanism, the network access points and the proxies that are to be used. 2. Send the provisioning document with the configuration context from the provisioning server a client. The server sends the document via WAP CL push with the default push port , the default application ID and the provisioning MIME-type (application/vnd.wap.connectivity-wbxml) to the client. (ProvBoot-B-C-001 and ProvBoot-B-C-011) 3. Select to save the configuration context on the client if necessary. 4. Check that the configuration context was received correctly.
Pass-Criteria	1. The client is authenticated using the network level validation by the server.

	2. The server is authenticated by the client.
	3. The client is able to save the received configuration context.
	4. The client received the configuration context correctly.

6.1.2   Using USERPIN Authentication Mechanism

Test Case Id	ClientProvisioning-1.1-int-001b
Test Object	Client and Server device
Test Case Description	Purpose of this verification is to ensure that a server and a client are able to communicate the mandatory initial connectivity information: basic transport connectivity information that includes parameters for network access points and the proxies that are to be used. USERPIN authentication mechanism shall be used.
Specification Reference	[PROVBOOT] Chapters 4.1 and 5 [PROVUAB] Chapters 4.1 and 4.2 [PROVCONT] Chapters 4.6.8 and 4.6.15
SCR Reference	ProvBoot-B-C-008 ProvBoot-B-C-011 ProvUAB-UDP-C-001 ProvUAB-UDP-C-002 ProvUAB-UDP-C-003 ProvUAB-UDP-C-006 ProvUAB-UDP-C-010 ProvUAB-UDP-C-011 ProvUAB-UDP-C-012 ProvUAB-UDP-C-013 ProvUAB-UDP-C-014 ProvUAB-UDP-C-015 ProvUAB-UEH-C-002 ProvCont-CC-C-001 ProvCont-CC-C-002 ProvCont-CC-C-004 ProvCont-CC-C-006 ProvCont-CC-C-015 ProvCont-CC-C-001 ProvBoot-BSF-C-002
Preconditions	▪ A Client Provisioning client to be configured. The client must have at least one network bearer. ▪ A Client Provisioning server connected to the internet. ▪ The receiving end doesn't have existing bootstrap context i.e. client is in unconfigured state.
Test Procedure	1. Create a configuration context on the provisioning server including the parameters for USERPIN security mechanism, the network access points and the proxies that are to be used. 2. Send the provisioning document with the configuration context from the provisioning server to a client. The server sends the document via WAP CL push with the default push port , the default application ID and the provisioning MIME-type (application/vnd.wap.connectivity-wbxml) to the client. (ProvBoot-B-C-001 and ProvBoot-B-C-011) 3. Select to save the configuration context on the client if necessary. 4. Check that the configuration context was received correctly.
Pass-Criteria	1. The client is authenticated using the network level validation by the server.

	2. The server is authenticated by the client.
	3. The client is able to save the received configuration context.
	4. The client received the configuration context correctly.

6.1.3 Using USERNETWPIN Authentication Mechanism

Test Case Id	ClientProvisioning-1.1-int-001c
Test Object	Client and Server device
Test Case Description	Purpose of this verification is to ensure that a server and a client are able to communicate the mandatory initial connectivity information: basic transport connectivity information that includes parameters for network access points and the proxies that are to be used. . USERNETWPIN authentication mechanism shall be used.
Specification Reference	[PROVBOOT] Chapters 4.1 and 5 [PROVUAB] Chapters 4.1 and 4.2 [PROVCONT] Chapters 4.6.8 and 4.6.15
SCR Reference	ProvBoot-B-C-008 ProvBoot-B-C-011 ProvUAB-UDP-C-001 ProvUAB-UDP-C-002 ProvUAB-UDP-C-003 ProvUAB-UDP-C-006 ProvUAB-UDP-C-010 ProvUAB-UDP-C-011 ProvUAB-UDP-C-012 ProvUAB-UDP-C-013 ProvUAB-UDP-C-014 ProvUAB-UDP-C-015 ProvUAB-UEH-C-002 ProvCont-CC-C-001 ProvCont-CC-C-002 ProvCont-CC-C-004 ProvCont-CC-C-006 ProvCont-CC-C-015 ProvCont-CC-C-001 ProvBoot-BSF-C-003
Preconditions	▪ A Client Provisioning client to be configured. The client must have at least one network bearer. ▪ A Client Provisioning server connected to the internet. ▪ The receiving end doesn't have existing bootstrap context i.e. client is in unconfigured state.
Test Procedure	1. Create a configuration context on the provisioning server including the parameters for USERNETWPIN security mechanism, the network access points and the proxies that are to be used. 2. Send the provisioning document with the configuration context from the provisioning server to a client. The server sends the document via WAP CL push with the default push port , the default application ID and the provisioning MIME-type (application/vnd.wap.connectivity-wbxml) to the client. (ProvBoot-B-C-001 and ProvBoot-B-C-011) 3. Select to save the configuration context on the client if necessary. 4. Check that the configuration context was received correctly.
Pass-Criteria	1. The client is authenticated using the network level validation by the server.

	2. The server is authenticated by the client.
	3. The client is able to save the received configuration context.
	4. The client received the configuration context correctly.

6.1.4   Using USERPINMAC Authentication Mechanism

Test Case Id	ClientProvisioning-1.1-int-001d
Test Object	Client and Server device
Test Case Description	Purpose of this verification is to ensure that a server and a client are able to communicate the mandatory initial connectivity information: basic transport connectivity information that includes parameters for network access points and the proxies that are to be used. USERPINMAC authentication mechanism shall be used.
Specification Reference	[PROVBOOT] Chapters 4.1 and 5 [PROVUAB] Chapters 4.1 and 4.2 [PROVCONT] Chapters 4.6.8 and 4.6.15
SCR Reference	ProvBoot-B-C-008 ProvBoot-B-C-011 ProvUAB-UDP-C-001 ProvUAB-UDP-C-002 ProvUAB-UDP-C-003 ProvUAB-UDP-C-006 ProvUAB-UDP-C-010 ProvUAB-UDP-C-011 ProvUAB-UDP-C-012 ProvUAB-UDP-C-013 ProvUAB-UDP-C-014 ProvUAB-UDP-C-015 ProvUAB-UEH-C-002 ProvCont-CC-C-001 ProvCont-CC-C-002 ProvCont-CC-C-004 ProvCont-CC-C-006 ProvCont-CC-C-015 ProvCont-CC-C-001 ProvBoot-BSF-C-004
Preconditions	▪ A Client Provisioning client to be configured. The client must have at least one network bearer. ▪ A Client Provisioning server connected to the internet. ▪ The receiving end doesn't have existing bootstrap context i.e. client is in unconfigured state.
Test Procedure	1. Create a configuration context on the provisioning server including the parameters for USERPINMAC security mechanism, the network access points and the proxies that are to be used. 2. Send the provisioning document with the configuration context from the provisioning server to a client. The server sends the document via WAP CL push with the default push port , the default application ID and the provisioning MIME-type (application/vnd.wap.connectivity-wbxml) to the client. (ProvBoot-B-C-001 and ProvBoot-B-C-011) 3. Select to save the configuration context on the client if necessary. 4. Check that the configuration context was received correctly.
Pass-Criteria	1. The client is authenticated using the network level validation by the server.

	2. The server is authenticated by the client.
	3. The client is able to save the received configuration context.
	4. The client received the configuration context correctly.

6.2   Bootstrap – Application settings, OTA

Test Case Id	ClientProvisioning-1.1-int-002
Test Object	Client and Server device
Test Case Description	Purpose of this verification is to ensure that a server and a client are able to communicate application settings (e.g. MMS).
Specification Reference	[PROVBOOT] Chapters 4.1 and 5 [PROVUAB] Chapters 4.1 and 4.2 [PROVCONT] Chapters 4.6.8 and 4.6.15
SCR Reference	ProvBoot-B-C-008 ProvUAB-UDP-C-014 ProvBoot-B-C-011 ProvUAB-UDP-C-015 ProvUAB-UDP-C-001 ProvUAB-UEH-C-002 ProvUAB-UDP-C-002 ProvCont-CC-C-001 ProvUAB-UDP-C-003 ProvCont-CC-C-002 ProvUAB-UDP-C-006 ProvCont-CC-C-004 ProvUAB-UDP-C-010 ProvCont-CC-C-006 ProvUAB-UDP-C-011 ProvCont-CC-C-015 ProvUAB-UDP-C-012 ProvCont-CC-C-001 ProvUAB-UDP-C-013
Preconditions	▪ A Client Provisioning client to be configured. The client must have at least one network bearer. ▪ A Client Provisioning server connected to the internet. ▪ The receiving end doesn't have existing bootstrap context.
Test Procedure	1. Create a particular configuration context on the provisioning server including application settings (e.g. MMS). 2. Send the provisioning document from the provisioning server to a client. 3. Select to save the configuration context on the client if necessary. 4. Check that the configuration context was received correctly.
Pass-Criteria	1. The client is authenticated using the network level validation by the server. 2. The server is authenticated by the client. 3. The client is able to save the received configuration context. 4. The client received the configuration context correctly.

6.3 Bootstrap – Multiple application settings in one configuration context, OTA

Test Case Id	ClientProvisioning-1.1-int-003	
Test Object	Client and Server device	
Test Case Description	Purpose of this verification is to ensure that a server and a client are able to communicate multiple (2+) application settings (e.g. Browser, MMS, Email, DM, DS, WVStreaming) inside one configuration context.	
Specification Reference	[PROVBOOT] Chapters 4.1 and 5 [PROVUAB] Chapters 4.1 and 4.2 [PROVCONT] Chapters 4.6.8 and 4.6.15	
SCR Reference	ProvBoot-B-C-008 ProvBoot-B-C-011 ProvUAB-UDP-C-001 ProvUAB-UDP-C-002 ProvUAB-UDP-C-003 ProvUAB-UDP-C-006 ProvUAB-UDP-C-010 ProvUAB-UDP-C-011 ProvUAB-UDP-C-012 ProvUAB-UDP-C-013	ProvUAB-UDP-C-014 ProvUAB-UDP-C-015 ProvUAB-UEH-C-002 ProvCont-CC-C-001 ProvCont-CC-C-002 ProvCont-CC-C-004 ProvCont-CC-C-006 ProvCont-CC-C-015 ProvCont-CC-C-001
Preconditions	▪ A Client Provisioning client to be configured. The client must have at least one network bearer. ▪ A Client Provisioning server connected to the internet. ▪ The receiving end doesn't have existing bootstrap context.	
Test Procedure	1. In the provisioning server, send the provisioning document CP_Prov_doc_1.xml from the provisioning server to a client. 2. Select to save the configuration context on the client if necessary. 3. Check that the configuration context was received correctly.	
Pass-Criteria	1. The client is authenticated using the network level validation by the server. 2. The server is authenticated by the client. 3. The client is able to save the received configuration context. 4. The client received the configuration context correctly. 5. All configuration parameters for the application settings defined in the XML document (CP_Prov_doc_1.xml) and supported by the client are correctly set. Unsupported application settings shall be ignored.	

6.4 Bootstrap – Multiple configuration contexts, OTA

Test Case Id	ClientProvisioning-1.1-int-004
Test Object	Client and Server device
Test Case Description	Purpose of this verification is to ensure that a server and a client are able to communicate multiple configuration contexts.
Specification Reference	[PROVBOOT] Chapters 4.1 and 5 [PROVUAB] Chapters 4.1, 4.2 and 8 [PROVCONT] Chapters 4.6.8 and 4.6.15
SCR Reference	ProvBoot-B-C-007 ProvBoot-B-C-008 ProvBoot-B-C-009 ProvBoot-B-C-010 ProvBoot-B-C-011 ProvUAB-UDP-C-001 ProvUAB-UDP-C-002 ProvUAB-UDP-C-003 ProvUAB-UDP-C-006 ProvUAB-UDP-C-010 ProvUAB-UDP-C-011 ProvUAB-UDP-C-012 ProvUAB-UDP-C-013 ProvUAB-UDP-C-014 ProvUAB-UDP-C-015 ProvUAB-UEH-C-002 ProvCont-CC-C-001 ProvCont-CC-C-002 ProvCont-CC-C-004 ProvCont-CC-C-006 ProvCont-CC-C-015 ProvCont-CC-C-001
Preconditions	▪ A Client Provisioning client to be configured. The client must have at least one network bearer. ▪ A Client Provisioning server connected to the internet. ▪ Client accepts more than one configuration context. The receiving end doesn't have existing bootstrap context.
Test Procedure	1. In the provisioning server, send the provisioning document CP_Prov_doc_1.xml from the provisioning server to a client. 2. Select to save the configuration context on the client if necessary. 3. Check that the configuration context was received correctly. 4. In the provisioning server, send CP_Prov_doc_2.xml (with different application settings than in the first phase) to a client. 5. Select to save the configuration context on the client if necessary. 6. Check that the second configuration context was received correctly.
Pass-Criteria	1. The client is authenticated using the network level validation by the server. 2. The server is authenticated by the client. 3. The client is able to save the received configuration context. 4. The client received both configuration contexts correctly. 5. All configuration parameters for the application settings defined in the XML documents (CP_Prov_doc_1.xml and CP_Prov_doc_2.xml) and supported by the client are correctly set. Unsupported application settings shall be ignored

6.5 Privileged configuration context, OTA

Test Case Id	ClientProvisioning-1.1-int-005
Test Object	Client and Server device
Test Case Description	Purpose of this verification is to ensure that a client is able to support privileged configuration context discarding new incoming configuration contexts when the provisioning document only allows one configuration context.
Specification Reference	[PROVBOOT] Chapters 5 [PROVUAB] Chapters 4.1, 4.2 and 8 [PROVCONT] Chapters 4.6.8 and 4.6.15
SCR Reference	ProvBoot-B-C-008 ProvUAB-UDP-C-012 ProvBoot-B-C-011 ProvUAB-UDP-C-013 ProvBoot-BGSM-C-014 ProvUAB-UDP-C-014 ProvBoot-BCDMA-C-006 ProvUAB-UDP-C-015 ProvBoot-BTDMA-C-005 ProvUAB-UEH-C-002 ProvUAB-UCM-C-001 ProvCont-CC-C-001 ProvUAB-UDP-C-001 ProvCont-CC-C-002 ProvUAB-UDP-C-002 ProvCont-CC-C-004 ProvUAB-UDP-C-003 ProvCont-CC-C-006 ProvUAB-UDP-C-006 ProvCont-CC-C-015 ProvUAB-UDP-C-010 ProvCont-CC-C-001 ProvUAB-UDP-C-011
Preconditions	▪ A Client Provisioning client to be configured. The client must have at least one network bearer. ▪ A Client Provisioning server connected to the Internet. ▪ The receiving end doesn't have an existing existent configuration context.
Test Procedure	1. Create a provisioning document configuration context on the provisioning server that allows only the privileged configuration context including the parameters for the network access points, the bearer, and the proxies. 2. In the provisioning server, send Bootstrap_zero.xml to the client. 3. On the client, select to save the initial configuration context sent from the provisioning server on the client if necessary. 4. Check that the privileged content cannot be modified on the client. (Note: However the user MAY make additions to the privileged context, for example userID and password, and the user can modify this information that has been defined by the user.) 5. Check that the configuration context was received correctly. 6. In the provisioning server, send CP_Prov_doc_2.xml to the client.

	7. The client discards the new configuration context
Pass-Criteria	1. The client is authenticated using the network level validation by the server.
	2. The server is authenticated by the client.
	3. The client is able to save the received configuration context (Bootstrap_zero.xml) .
	4. The client received the configuration context correctly.
	5. The client user is not able to modify the content of the configuration context.
	6. The client discards additional configuration context other than the first.

6.6   Bootstrap, Smart Card

Test Case Id	ClientProvisioning-1.1-int-006	
Test Object	Client and Server device	
Test Case Description	Purpose of this verification is to ensure that the client can use of the connectivity and application information that is pre-stored within smart card.	
Specification Reference	[PROVBOOT] Chapters 4 [PROVUAB] Chapter 5.1 [PROVSC] Chapters 5.1 [PROVCONT] Chapters 4.6.8 and 4.6.15	
SCR Reference	PROVSC-ICC-001 PROVSC-C-001 ProvBoot-B-C-001 ProvBoot-B-C-008 ProvCont-CC-C-001	ProvCont-CC-C-002 ProvCont-CC-C-004 ProvCont-CC-C-006 ProvCont-CC-C-015 ProvCont-CC-C-001
Preconditions	▪ A Client Provisioning client to be configured ▪ A smart card with provisioning content ▪ The Client Provisioning client doesn't have existing bootstrap context.	
Test Procedure	1. Insert a smart card to the mobile terminal. 2. Select to configure the terminal from the Smart Card if necessary. 3. On the client, select to save the initial configuration context read from the Smart Card on the client if necessary. 4. Check that the connectivity information is saved in the client. 5. Check that the client can use the configuration context correctly.	
Pass-Criteria	1. The client is able to save the bootstrap configuration correctly from the smart card.	

	2. The client received the configuration context correctly.

6.7   Modification of a configuration context, Smart Card

Test Case Id	ClientProvisioning-1.1-int-007	
Test Object	Client and Smart Card	
Test Case Description	Purpose of this verification is to ensure that the client can modify connectivity and the application information that is pre-stored within smart card in Config1 and Config2 files.	
Specification Reference	[PROVBOOT] Chapters 4 [PROVUAB] Chapter 5.1 [PROVSC] Chapters 5.1 [PROVCONT] Chapters 4.6.8 and 4.6.15	
SCR Reference	PROVSC-ICC-001 PROVSC-C-001 PROVSC-WIM-103 PROVSC-WIM-104 PROVSC-WIM-105 PROVSC-WIM-106 PROVSC-SIM-105 PROVSC-SIM-106 PROVSC-SIM-107 PROVSC-SIM-108 PROVSC-UICC-106	PROVSC-UICC-107 PROVSC-UICC-108 PROVSC-UICC-109 ProvBoot-B-C-001 ProvBoot-B-C-008 ProvCont-CC-C-001 ProvCont-CC-C-002 ProvCont-CC-C-004 ProvCont-CC-C-006 ProvCont-CC-C-015 ProvCont-CC-C-001
Preconditions	▪ A Client Provisioning client to be configured. ▪ A smart card with provisioning content ▪ The Client Provisioning client has existing context already.	
Test Procedure	1. Check that the smart card has connectivity and the application information (e.g. MMS settings, GPRS settings) in Config1 and Config2 files. 2. Select on the client to read the connectivity and the application information stored in Config1 file. 3. Modify one of the connectivity parameters (e.g. Authentication ID, password) in the Config1 file by entering the correct enabled PIN. 4. Check that the client can use the configuration context in the Config1 file correctly. 5. Select on the client to read the connectivity and the application information stored in Config2 file. 6. Modify one of the connectivity parameters (e.g. Authentication ID, password) in the Config2 file. 7. Check that the client can use the configuration context in the Config2 file correctly.	

| Pass-Criteria | 1. The client is able to read the connectivity and the application information stored in Config1 and Config2 files correctly. |
| | 2. The client can edit connectivity parameters stored in Config1 and Config2 files on the smart card. |

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-ETS-ClientProvisioning-v1_1	16 Dec 2003	Initial document Ref TP Doc# OMA-TP-2003-0647 -Client-Provisioning-1.1-Enabler-test-specification-for-approval
	14 Apr 2005	Ref Doc# OMA-ETS-ClientProvisioning-v1_1-20050414-D approved by IOP WG.
	22 Jul 2005	Ref Doc# OMA-TP-2005-0223R01-Update-of-CP_1_1-ETS

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Version OMA-ETS-ClientProvisioning-v1_1	21 Feb 2008	6.5	CR incorporated: OMA-IOP-MEC-2008-0052
Candidate Version OMA-ETS-ClientProvisioning-v1_1	21 Mar 2008	n/a	TP Notification Ref Doc# OMA-TP-2008-0073R01-INP_CP_1.1_ETS_for_Notification

Appendix B.   Reference Configuration Messages (Normative)

B.1   UAB tests doc.xml

<?xml version="1.0"?>

<!DOCTYPE wap-provisioningdoc PUBLIC "-//WAPFORUM//DTD PROV 1.0//EN" "http://www.wapforum.org/DTD/prov.dtd">

<wap-provisioningdoc version="1.0">

 <characteristic type="PXLOGICAL">

  <parm name="PROXY-ID" value="www.operator.com"/>

  <parm name="NAME" value="Gateway WAP"/>

   <!-- UNKNOWN PARAMETER -->

  <parm name="unknown_parameter" value="http://wap.operator.com"/>

  <characteristic type="PXPHYSICAL">

   <parm name="PHYSICAL-PROXY-ID" value="PROXY_WAP_1"/>

   <parm name="PXADDR" value="10.138.255.129"/>

   <parm name="PXADDRTYPE" value="IPV4"/>

   <!-- PXPHYSICAL WITHOUT NAP DEFINED -->

   <characteristic type="PORT">

    <parm name="PORTNBR" value="8080"/>

   </characteristic>

  </characteristic>

  <characteristic type="PXPHYSICAL">

   <parm name="PHYSICAL-PROXY-ID" value="PROXY_WAP_2"/>

   <parm name="PXADDR" value="192.168.80.21"/>

   <parm name="PXADDRTYPE" value="IPV4"/>

   <parm name="TO-NAPID" value="WAP_GPRS"/>

   <parm name="TO-NAPID" value="WAP_CSD"/>

  </characteristic>

  <!-- PXPHYSICAL DEFINED MULTIPLE TIMES -->

  <characteristic type="PXPHYSICAL">

   <parm name="PHYSICAL-PROXY-ID" value="PROXY_WAP_2"/>

   <parm name="PXADDR" value="172.121.89.56"/>

   <parm name="PXADDRTYPE" value="IPV4"/>

   <parm name="TO-NAPID" value="WAP_GPRS"/>

   <parm name="TO-NAPID" value="WAP_CSD"/>

```
    <characteristic type="PORT">

     <parm name="PORTNBR" value="8080"/>

     </characteristic>

   </characteristic>


 </characteristic>


   <!-- PXLOGICAL DEFINED MULTIPLE TIMES -->

 <characteristic type="PXLOGICAL">

  <parm name="PROXY-ID" value="www.operator.com"/>

  <parm name="NAME" value="GW WAP"/>

  <characteristic type="PXPHYSICAL">

   <parm name="PHYSICAL-PROXY-ID" value="PROXY_WAP_3"/>

   <parm name="PXADDR" value="172.150.70.5"/>

   <parm name="PXADDRTYPE" value="IPV4"/>

   <parm name="TO-NAPID" value="WAP_GPRS"/>

   <parm name="TO-NAPID" value="WAP_CSD"/>

  </characteristic>

 </characteristic>



 <characteristic type="NAPDEF">

  <parm name="NAPID" value="WAP_GPRS"/>

  <parm name="BEARER" value="GSM-GPRS"/>

  <parm name="NAME" value="operator GPRS"/>

  <parm name="NAP-ADDRESS" value="wap.operator.com"/>

  <parm name="NAP-ADDRTYPE" value="APN"/>

  <characteristic type="NAPAUTHINFO">

   <parm name="AUTHTYPE" value="PAP"/>

   <parm name="AUTHNAME" value="WAPOP"/>

   <parm name="AUTHSECRET" value="WAPOP"/>

  </characteristic>

 </characteristic>

 <!-- MULTIPLE NAP DEFINITIONS -->

 <characteristic type="NAPDEF">

  <parm name="NAPID" value="WAP_GPRS"/>
```

```
<parm name="BEARER" value="GSM-GPRS"/>

<parm name="NAME" value="operator GPRS"/>

<parm name="NAP-ADDRESS" value="wapOP.operator.com"/>

<parm name="NAP-ADDRTYPE" value="APN"/>

<characteristic type="NAPAUTHINFO">

  <parm name="AUTHTYPE" value="PAP"/>

  <parm name="AUTHNAME" value="WAPOP"/>

  <parm name="AUTHSECRET" value="WAPOP"/>

</characteristic>

</characteristic>

<!-- NAP DEFINITION WITH BEARER NOT SUPPORTED -->

<characteristic type="NAPDEF">

 <parm name="NAPID" value="WAP_CSD"/>

 <parm name="BEARER" value="unknown_bearer"/>

 <parm name="NAME" value="operator CSD"/>

 <parm name="NAP-ADDRESS" value="+34629000556"/>

 <parm name="NAP-ADDRTYPE" value="E164"/>

 <parm name="CALLTYPE" value="ANALOG-MODEM"/>

 <parm name="LINKSPEED" value="AUTOBAUDING"/>

 <characteristic type="NAPAUTHINFO">

  <parm name="AUTHTYPE" value="PAP"/>

  <parm name="AUTHNAME" value="WAPOP"/>

  <parm name="AUTHSECRET" value="WAPOP"/>

 </characteristic>

</characteristic>


<characteristic type="NAPDEF">

 <parm name="NAPID" value="Internet_GPRS"/>

 <parm name="BEARER" value="GSM-GPRS"/>

 <parm name="NAME" value="Operator Internet GPRS"/>

 <parm name="INTERNET"/>

 <parm name="NAP-ADDRESS" value="operator.com"/>

 <parm name="NAP-ADDRTYPE" value="APN"/>

 <parm name="DNS-ADDR" value="194.179.1.100"/>

 <parm name="DNS-ADDR" value="194.179.1.101"/>

 <characteristic type="NAPAUTHINFO">
```

```
    <parm name="AUTHTYPE" value="PAP"/>

    <parm name="AUTHNAME" value="OPERATOR"/>

    <parm name="AUTHSECRET" value="OPERATOR"/>

   </characteristic>

 </characteristic>




<!-- APPLICATION characteristic for WAP Browser -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="w2"/>

 <parm name="NAME" value="Operator-portal"/>

 <parm name="TO-PROXY" value="www.operator.com"/>

 <parm name="TO-NAPID" value="Internet_GPRS"/>

 <characteristic type="RESOURCE">

  <parm name="URI" value="http://wap.operator_portal.com"/>

  <parm name="NAME" value="Operator portal"/>

  <parm name="STARTPAGE"/>

 </characteristic>

</characteristic>




 <!-- APPLICATION characteristic for WAP Browser: REDUNDANT CHARACTERISTIC -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="w2"/>

 <parm name="NAME" value="Operator-portal"/>

 <parm name="TO-PROXY" value="www.wap.operator.com"/>

 <parm name="TO-NAPID" value="Internet_GPRS"/>

</characteristic>




<!-- APPLICATION characteristic for MMS -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="w4"/>

 <parm name="TO-NAPID" value="OP_MMS"/>

 <parm name="ADDR" value="http://mms.operator.com"/>

 <!-- REDUNDANT PARAMETER -->

 <parm name="ADDR" value="http://mms_proxy.operator.com"/>
```

```
  </characteristic>


  <characteristic type="NAPDEF">

    <parm name="NAPID" value="OP_MMS"/>

    <parm name="BEARER" value="GSM-GPRS"/>

    <parm name="NAME" value="Operator MMS"/>

    <parm name="NAP-ADDRESS" value="mms.operator.com"/>

    <parm name="NAP-ADDRTYPE" value="APN"/>

    <characteristic type="NAPAUTHINFO">

      <parm name="AUTHTYPE" value="PAP"/>

      <parm name="AUTHNAME" value="OPERATOR@mms"/>

      <parm name="AUTHSECRET" value="OPERATOR"/>

    </characteristic>

  </characteristic>


  <!-- UNKNOWN CHARACTERISTIC -->

  <characteristic type="unknown_characteristic">

    <parm name="APPID" value="554"/>

    <parm name="NAME"  value="unknown"/>

    <parm name="TO-PROXY" value="Proxy_unknown"/>

  </characteristic>


  <!-- UNKNOWN VALUE -->

  <characteristic type="APPLICATION">

    <parm name="APPID" value="7464587964"/>

    <parm name="NAME"  value="New Application"/>

    <parm name="TO-PROXY" value="Proxy_NewApplication"/>

  </characteristic>


</wap-provisioningdoc>
```

B.2 CP_Prov_doc_1.xml

```
<?xml version="1.0"?>

<!DOCTYPE wap-provisioningdoc PUBLIC "-//WAPFORUM//DTD PROV 1.0//EN" "http://www.wapforum.org/DTD/prov.dtd">

<wap-provisioningdoc version="1.0">


<!-- BOOTSTRAP characteristic -->

                  <characteristic type="BOOTSTRAP">

                   <parm name="NAME" value="Operator"/>

       <parm name="CONTEXT-ALLOW" value="255"/>

                    </characteristic>



<!-- Connectivities Definition -->

 <characteristic type="PXLOGICAL">

  <parm name="PROXY-ID" value="www.operator.com"/>

  <parm name="NAME" value="Gateway WAP"/>

  <parm name="STARTPAGE" value="http://wap.operator.com"/>


  <characteristic type="PXPHYSICAL">

   <parm name="PHYSICAL-PROXY-ID" value="PROXY_WAP_1"/>

   <parm name="PXADDR" value="10.138.255.129"/>

   <parm name="PXADDRTYPE" value="IPV4"/>

   <parm name="TO-NAPID" value="WAP_GPRS"/>

   <parm name="TO-NAPID" value="WAP_CSD"/>

   <characteristic type="PORT">

    <parm name="PORTNBR" value="8080"/>

   </characteristic>

  </characteristic>


  <characteristic type="PXPHYSICAL">

   <parm name="PHYSICAL-PROXY-ID" value="PROXY_WAP_2"/>

   <parm name="PXADDR" value="192.168.80.21"/>

   <parm name="PXADDRTYPE" value="IPV4"/>

   <parm name="TO-NAPID" value="WAP_GPRS"/>

   <parm name="TO-NAPID" value="WAP_CSD"/>
```

```
<characteristic type="PORT">

  <parm name="PORTNBR" value="8080"/>

 </characteristic>

</characteristic>


</characteristic>


<characteristic type="NAPDEF">

 <parm name="NAPID" value="WAP_GPRS"/>

 <parm name="BEARER" value="GSM-GPRS"/>

 <parm name="NAME" value="operator GPRS"/>

 <parm name="NAP-ADDRESS" value="wap.operator.com"/>

 <parm name="NAP-ADDRTYPE" value="APN"/>

 <characteristic type="NAPAUTHINFO">

  <parm name="AUTHTYPE" value="PAP"/>

  <parm name="AUTHNAME" value="WAPOP"/>

  <parm name="AUTHSECRET" value="WAPOP"/>

 </characteristic>

</characteristic>


<characteristic type="NAPDEF">

 <parm name="NAPID" value="WAP_CSD"/>

 <parm name="BEARER" value="GSM-CSD"/>

 <parm name="NAME" value="operator CSD"/>

 <parm name="NAP-ADDRESS" value="+34629000556"/>

 <parm name="NAP-ADDRTYPE" value="E164"/>

 <parm name="CALLTYPE" value="ANALOG-MODEM"/>

 <parm name="LINKSPEED" value="AUTOBAUDING"/>

 <characteristic type="NAPAUTHINFO">

  <parm name="AUTHTYPE" value="PAP"/>

  <parm name="AUTHNAME" value="WAPOP"/>

  <parm name="AUTHSECRET" value="WAPOP"/>

 </characteristic>

</characteristic>


<characteristic type="NAPDEF">
```

```
<parm name="NAPID" value="Internet_GPRS"/>

<parm name="BEARER" value="GSM-GPRS"/>

<parm name="NAME" value="Operator Internet GPRS"/>

<parm name="INTERNET"/>

<parm name="NAP-ADDRESS" value="operator.com"/>

<parm name="NAP-ADDRTYPE" value="APN"/>

<parm name="DNS-ADDR" value="194.179.1.100"/>

<parm name="DNS-ADDR" value="194.179.1.101"/>

<characteristic type="NAPAUTHINFO">

  <parm name="AUTHTYPE" value="PAP"/>

  <parm name="AUTHNAME" value="OPERATOR"/>

  <parm name="AUTHSECRET" value="OPERATOR"/>

</characteristic>

</characteristic>



<!-- APPLICATION characteristic for WAP Browser -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="w2"/>

 <parm name="NAME" value="Operator-portal"/>

 <parm name="TO-PROXY" value="www.operator.com"/>

 <parm name="TO-NAPID" value="Internet_GPRS"/>

 <characteristic type="RESOURCE">

  <parm name="URI" value="http://wap.operator_portal.com"/>

  <parm name="NAME" value="Operator portal"/>

  <parm name="STARTPAGE"/>

 </characteristic>

</characteristic>



<!-- APPLICATION characteristic for MMS -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="w4"/>

 <parm name="TO-NAPID" value="OP_MMS"/>

 <parm name="ADDR" value="http://mms.operator.com"/>

</characteristic>
```

```xml
<characteristic type="NAPDEF">

  <parm name="NAPID" value="OP_MMS"/>

  <parm name="BEARER" value="GSM-GPRS"/>

  <parm name="NAME" value="Operator MMS"/>

  <parm name="NAP-ADDRESS" value="mms.operator.com"/>

  <parm name="NAP-ADDRTYPE" value="APN"/>

  <characteristic type="NAPAUTHINFO">

   <parm name="AUTHTYPE" value="PAP"/>

   <parm name="AUTHNAME" value="OPERATOR@mms"/>

   <parm name="AUTHSECRET" value="OPERATOR"/>

  </characteristic>

</characteristic>


<!-- APPLICATION characteristic for DM -->

<characteristic type="APPLICATION">

  <parm name="APPID" value="w7"/>

  <parm name="PROVIDER-ID" value="DM Server ID"/>

  <parm name="NAME" value="DM Server"/>

  <parm name="ADDR" value="http://dm.operator.com"/>

  <parm name="TO-NAPID" value="Internet_GPRS"/>

  <characteristic type="APPAUTH">

   <parm name="AAUTHLEVEL" value="APPSRV"/>

   <parm name="AAUTHTYPE" value="DIGEST,BASIC"/>

   <parm name="AAUTHNAME" value="servername"/>

   <parm name="AAUTHSECRET" value="serversecret"/>

   <parm name="AAUTHDATA" value="servernonce"/>

  </characteristic>

  <characteristic type="APPAUTH">

   <parm name="AAUTHLEVEL" value="CLIENT"/>

   <parm name="AAUTHNAME" value="clientname"/>

   <parm name="AAUTHSECRET" value="clientsecret"/>

   <parm name="AAUTHDATA" value="clientnonce"/>

  </characteristic>

</characteristic>
```

```
<!-- APPLICATION characteristic for SMTP -->
<characteristic type="APPLICATION">
 <parm name="APPID" value="25"/>
 <parm name="PROVIDER-ID" value="Operator e-mail"/>
 <parm name="NAME" value="Operator Mail"/>
 <parm name="TO-NAPID" value="Internet_GPRS"/>
 <parm name="FROM" value="MSISDN@operator.com"/>
 <characteristic type="APPADDR">
  <parm name="ADDR" value="smtp.operator.com"/>
  <characteristic type="PORT">
   <parm name="PORTNBR" value="25"/>
   <parm name="SERVICE" value="STARTTLS"/>
  </characteristic>
 </characteristic>
 <characteristic type="APPAUTH">
  <parm name="AAUTHNAME" value="MSISDN"/>
  <parm name="AAUTHSECRET" value="password"/>
 </characteristic>
</characteristic>


<!-- APPLICATION characteristic for POP3 -->
<characteristic type="APPLICATION">
 <parm name="APPID" value="110"/>
 <parm name="PROVIDER-ID" value="Operator e-mail"/>
 <parm name="NAME" value="Operator Mail"/>
 <parm name="TO-NAPID" value="Internet_GPRS"/>
 <characteristic type="APPADDR">
  <parm name="ADDR" value="pop3.operator.com"/>
  <characteristic type="PORT">
   <parm name="PORTNBR" value="110"/>
   <parm name="SERVICE" value="STARTTLS"/>
  </characteristic>
 </characteristic>
 <characteristic type="APPAUTH">
  <parm name="AAUTHNAME" value="MSISDN"/>
```

```xml
    <parm name="AAUTHSECRET" value="password"/>

  </characteristic>

</characteristic>


<!-- APPLICATION for IMAP services -->

<characteristic type="APPLICATION">

                <parm name="APPID" value="143"/>

                <parm name="PROVIDER-ID" value="MyMail"/>

                <parm name="TO-NAPID" value="Internet_GPRS"/>

                <characteristic type="APPADDR">

                <parm name="ADDR" value="imap.operator.com"/>

                <parm name="ADDRTYPE" value="ALPHA"/>

                  <characteristic type="PORT">

                  <parm name="PORTNBR" value="143"/>

                <parm name="SERVICE" value="STARTTLS"/>

                </characteristic>

                </characteristic>

                <characteristic type="APPAUTH">

                <parm name="AAUTHTYPE" value="CRAM-MD5"/>

                <parm name="AAUTHNAME" value="username"/>

                <parm name="AAUTHSECRET" value="password"/>

                </characteristic>

                </characteristic>


<!-- APPLICATION characteristic for Streaming -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="554"/>

 <parm name="NAME"  value="Streaming"/>

 <parm name="TO-PROXY" value="www.streaming.operator.com"/>

 <parm name="MIN-UDP-PORT" value="7000"/>

 <parm name="MAX-UDP-PORT" value="30000"/>

</characteristic>


<characteristic type="PXLOGICAL">

 <parm name="PROXY-ID" value="www.streaming.operator.com"/>

 <parm name="NAME" value="Proxy Streaming"/>
```

```
<characteristic type="PORT">

  <parm name="PORTNBR" value="8080"/>

</characteristic>

<characteristic type="PXPHYSICAL">

  <parm name="PHYSICAL-PROXY-ID" value="PROXY_STREAMING"/>

  <parm name="PXADDR" value="172.16.20.3"/>

  <parm name="PXADDRTYPE" value="IPV4"/>

  <parm name="TO-NAPID" value="Internet_GPRS"/>

</characteristic>

</characteristic>


</wap-provisioningdoc>
```

B.3 CP_Prov_doc_2.xml

<?xml version="1.0"?>

<!DOCTYPE wap-provisioningdoc PUBLIC "-//WAPFORUM//DTD PROV 1.0//EN" "http://www.wapforum.org/DTD/prov.dtd">

<wap-provisioningdoc version="1.0">

<!-- APPLICATION characteristic for Instant Message and Precense Service -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="wA"/>

 <parm name="NAME" value="IM"/>

 <parm name="ADDR" value="http://IMPSserver:port/path/path"/>

 <parm name="TO-NAPID" value="Internet_GPRS"/>

 <characteristic type="APPAUTH">

 <parm name="AAUTHNAME" value="authname"/>

 <parm name="AAUTHSECRET" value="authsecret"/>

 </characteristic>

 </characteristic>

<!-- APPLICATION characteristic for DS -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="w5"/>

 <parm name="NAME" value="SyncmlServ"/>

<!-- Server address -->

<parm name="ADDR" value="http://DSserver/syncml"/>

<parm name="TO-NAPID" value="Internet_GPRS"/>

 <!-- Contacts DB -->

 <characteristic type="RESOURCE">

 <parm name="URI" value="Contacts"/>

 <parm name="NAME" value="Contacts DB"/>

 <parm name="AACCEPT" value="text/x-vcard"/>

 </characteristic>

 <!-- Calendar DB -->

 <characteristic type="RESOURCE">

 <parm name="URI" value="Calendar"/>

 <parm name="NAME" value="Calendar DB"/>

```
  <parm name="AACCEPT" value="text/x-vcalendar"/>

 </characteristic>

 <!-- Notes DB -->

 <characteristic type="RESOURCE">

 <parm name="URI" value="NOTE"/>

 <parm name="NAME" value="NOTES DB"/>

 <parm name="AACCEPT" value="test/plain"/>

 </characteristic>


 <characteristic type="APPAUTH">

 <parm name="AAUTHNAME" value="authname"/>

 <parm name="AAUTHSECRET" value="authpass"/>

 </characteristic>

</characteristic>


<!-- APPLICATION for Push To Talk, PoC -->

 <characteristic type="APPLICATION">

                  <parm name="APPID" value="w9002"/>

                  <parm name="NAME" value="Operator - Push to Talk"/>

                  <parm name="TO-NAPID" value="Internet_GPRS"/>

                  <characteristic type="APPADDR">

                  <parm name="ADDR" value="123.123.123.123"/>

                  <parm name="ADDRTYPE" value="IPv4"/>

                  <characteristic type="PORT">

      <parm name="PORTNBR" value="8080"/>

                  </characteristic>

                  </characteristic>

                  <characteristic type="APPAUTH">

                  <parm name="AAUTHNAME" value="username"/>

                  <parm name="AAUTHSECRET" value="password"/>

                  <parm name="AAUTHDATA" value="binary data"/>

                  </characteristic>

                  </characteristic>


</wap-provisioningdoc>
```

B.4 Bootstrap_zero.xml

```
<?xml version="1.0"?>

<!DOCTYPE wap-provisioningdoc PUBLIC "-//WAPFORUM//DTD PROV 1.0//EN" "http://www.wapforum.org/DTD/prov.dtd">

<wap-provisioningdoc version="1.0">


<!-- BOOTSTRAP characteristic -->

                <characteristic type="BOOTSTRAP">

                 <parm name="NAME" value="Operator"/>

                                    <parm name="CONTEXT-ALLOW" value="0"/>

                </characteristic>


<characteristic type="PXLOGICAL">

 <parm name="PROXY-ID" value="www.operator.com"/>

 <parm name="NAME" value="Gateway WAP"/>

 <parm name="STARTPAGE" value="http://wap.operator.com"/>


<characteristic type="PXPHYSICAL">

 <parm name="PHYSICAL-PROXY-ID" value="PROXY_WAP_1"/>

 <parm name="PXADDR" value="10.138.255.129"/>

 <parm name="PXADDRTYPE" value="IPV4"/>

 <parm name="TO-NAPID" value="WAP_GPRS"/>

 <parm name="TO-NAPID" value="WAP_CSD"/>

 <characteristic type="PORT">

  <parm name="PORTNBR" value="8080"/>

 </characteristic>

</characteristic>


<characteristic type="PXPHYSICAL">

 <parm name="PHYSICAL-PROXY-ID" value="PROXY_WAP_2"/>

 <parm name="PXADDR" value="192.168.80.21"/>

 <parm name="PXADDRTYPE" value="IPV4"/>

 <parm name="TO-NAPID" value="WAP_GPRS"/>

 <parm name="TO-NAPID" value="WAP_CSD"/>

 <characteristic type="PORT">

  <parm name="PORTNBR" value="8080"/>

 </characteristic>
```

```
  </characteristic>


</characteristic>


<characteristic type="NAPDEF">
 <parm name="NAPID" value="WAP_GPRS"/>
 <parm name="BEARER" value="GSM-GPRS"/>
 <parm name="NAME" value="operator GPRS"/>
 <parm name="NAP-ADDRESS" value="wap.operator.com"/>
 <parm name="NAP-ADDRTYPE" value="APN"/>
 <characteristic type="NAPAUTHINFO">
  <parm name="AUTHTYPE" value="PAP"/>
  <parm name="AUTHNAME" value="WAPOP"/>
  <parm name="AUTHSECRET" value="WAPOP"/>
 </characteristic>
</characteristic>


<characteristic type="NAPDEF">
 <parm name="NAPID" value="WAP_CSD"/>
 <parm name="BEARER" value="GSM-CSD"/>
 <parm name="NAME" value="operator CSD"/>
 <parm name="NAP-ADDRESS" value="+34629000556"/>
 <parm name="NAP-ADDRTYPE" value="E164"/>
 <parm name="CALLTYPE" value="ANALOG-MODEM"/>
 <parm name="LINKSPEED" value="AUTOBAUDING"/>
 <characteristic type="NAPAUTHINFO">
  <parm name="AUTHTYPE" value="PAP"/>
  <parm name="AUTHNAME" value="WAPOP"/>
  <parm name="AUTHSECRET" value="WAPOP"/>
 </characteristic>
</characteristic>


<characteristic type="NAPDEF">
 <parm name="NAPID" value="Internet_GPRS"/>
 <parm name="BEARER" value="GSM-GPRS"/>
 <parm name="NAME" value="Operator Internet GPRS"/>
```

```
<parm name="INTERNET"/>

<parm name="NAP-ADDRESS" value="operator.com"/>

<parm name="NAP-ADDRTYPE" value="APN"/>

<parm name="DNS-ADDR" value="194.179.1.100"/>

<parm name="DNS-ADDR" value="194.179.1.101"/>

<characteristic type="NAPAUTHINFO">

  <parm name="AUTHTYPE" value="PAP"/>

  <parm name="AUTHNAME" value="OPERATOR"/>

  <parm name="AUTHSECRET" value="OPERATOR"/>

</characteristic>

</characteristic>



<!-- APPLICATION characteristic for WAP Browser -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="w2"/>

 <parm name="NAME" value="Operator-portal"/>

 <parm name="TO-PROXY" value="www.operator.com"/>

 <parm name="TO-NAPID" value="Internet_GPRS"/>

 <characteristic type="RESOURCE">

  <parm name="URI" value="http://wap.operator_portal.com"/>

  <parm name="NAME" value="Operator portal"/>

  <parm name="STARTPAGE"/>

 </characteristic>

</characteristic>



<!-- APPLICATION characteristic for MMS -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="w4"/>

 <parm name="TO-NAPID" value="OP_MMS"/>

 <parm name="ADDR" value="http://mms.operator.com"/>

</characteristic>



<characteristic type="NAPDEF">

 <parm name="NAPID" value="OP_MMS"/>

 <parm name="BEARER" value="GSM-GPRS"/>
```

```
<parm name="NAME" value="Operator MMS"/>

<parm name="NAP-ADDRESS" value="mms.operator.com"/>

<parm name="NAP-ADDRTYPE" value="APN"/>

<characteristic type="NAPAUTHINFO">

  <parm name="AUTHTYPE" value="PAP"/>

  <parm name="AUTHNAME" value="OPERATOR@mms"/>

  <parm name="AUTHSECRET" value="OPERATOR"/>

 </characteristic>

</characteristic>


<!-- APPLICATION characteristic for DM -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="w7"/>

 <parm name="PROVIDER-ID" value="DM Server ID"/>

 <parm name="NAME" value="DM Server"/>

 <parm name="ADDR" value="http://dm.operator.com"/>

 <parm name="TO-NAPID" value="Internet_GPRS"/>

 <characteristic type="APPAUTH">

  <parm name="AAUTHLEVEL" value="APPSRV"/>

  <parm name="AAUTHTYPE" value="DIGEST,BASIC"/>

  <parm name="AAUTHNAME" value="servername"/>

  <parm name="AAUTHSECRET" value="serversecret"/>

  <parm name="AAUTHDATA" value="servernonce"/>

 </characteristic>

 <characteristic type="APPAUTH">

  <parm name="AAUTHLEVEL" value="CLIENT"/>

  <parm name="AAUTHNAME" value="clientname"/>

  <parm name="AAUTHSECRET" value="clientsecret"/>

  <parm name="AAUTHDATA" value="clientnonce"/>

 </characteristic>

</characteristic>


<!-- APPLICATION characteristic for SMTP -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="25"/>

 <parm name="PROVIDER-ID" value="Operator e-mail"/>
```

```
<parm name="NAME" value="Operator Mail"/>

<parm name="TO-NAPID" value="Internet_GPRS"/>

<parm name="FROM" value="MSISDN@operator.com"/>

<characteristic type="APPADDR">

  <parm name="ADDR" value="smtp.operator.com"/>

  <characteristic type="PORT">

    <parm name="PORTNBR" value="25"/>

    <parm name="SERVICE" value="STARTTLS"/>

  </characteristic>

</characteristic>

<characteristic type="APPAUTH">

  <parm name="AAUTHNAME" value="MSISDN"/>

  <parm name="AAUTHSECRET" value="password"/>

</characteristic>

</characteristic>


<!-- APPLICATION characteristic for POP3 -->

<characteristic type="APPLICATION">

  <parm name="APPID" value="110"/>

  <parm name="PROVIDER-ID" value="Operator e-mail"/>

  <parm name="NAME" value="Operator Mail"/>

  <parm name="TO-NAPID" value="Internet_GPRS"/>

  <characteristic type="APPADDR">

    <parm name="ADDR" value="pop3.operator.com"/>

    <characteristic type="PORT">

      <parm name="PORTNBR" value="110"/>

      <parm name="SERVICE" value="STARTTLS"/>

    </characteristic>

  </characteristic>

  <characteristic type="APPAUTH">

    <parm name="AAUTHNAME" value="MSISDN"/>

    <parm name="AAUTHSECRET" value="password"/>

  </characteristic>

</characteristic>


<!-- APPLICATION for IMAP services -->
```

```
<characteristic type="APPLICATION">

                    <parm name="APPID" value="143"/>

                    <parm name="PROVIDER-ID" value="MyMail"/>

                    <parm name="TO-NAPID" value="Internet_GPRS"/>

                    <characteristic type="APPADDR">

                    <parm name="ADDR" value="imap.operator.com"/>

                    <parm name="ADDRTYPE" value="ALPHA"/>

                     <characteristic type="PORT">

                      <parm name="PORTNBR" value="143"/>

                    <parm name="SERVICE" value="STARTTLS"/>

                    </characteristic>

                    </characteristic>

                    <characteristic type="APPAUTH">

                    <parm name="AAUTHTYPE" value="CRAM-MD5"/>

                    <parm name="AAUTHNAME" value="username"/>

                    <parm name="AAUTHSECRET" value="password"/>

                    </characteristic>

                    </characteristic>


<!-- APPLICATION characteristic for Streaming -->

<characteristic type="APPLICATION">

 <parm name="APPID" value="554"/>

 <parm name="NAME"  value="Streaming"/>

 <parm name="TO-PROXY" value="www.streaming.operator.com"/>

 <parm name="MIN_UDP_PORT" value="7000"/>

 <parm name="MAX_UDP_PORT" value="30000"/>

</characteristic>


<characteristic type="PXLOGICAL">

 <parm name="PROXY-ID" value="www.streaming.operator.com"/>

 <parm name="NAME" value="Proxy Streaming"/>

 <characteristic type="PORT">

  <parm name="PORTNBR" value="8080"/>

 </characteristic>

 <characteristic type="PXPHYSICAL">

  <parm name="PHYSICAL-PROXY-ID" value="PROXY_STREAMING"/>
```

```
    <parm name="PXADDR" value="172.16.20.3"/>

    <parm name="PXADDRTYPE" value="IPV4"/>

    <parm name="TO-NAPID" value="Internet_GPRS"/>

  </characteristic>

 </characteristic>


</wap-provisioningdoc>
```