Provisioning Content

Candidate Version 1.1 – 26 Feb 2008

Open Mobile Alliance

OMA-WAP-TS-ProvCont-v1_1-20080226-C

Continues the Technical Activities
Originated in the WAP Forum

Contents

1. Scope

The Wireless Application Protocol (WAP) is a result of continuous work to define an industry-wide specification for developing applications that operate over wireless communication networks. The Open Mobile Alliance continues the work of the WAP Forum to define a set of specifications to be used by service applications. For information on the WAP architecture, please refer to "*Wireless Application Protocol Architecture Specification"* [WAPARCH].

Provisioning is the process by which a WAP client is configured with a minimum of user interaction. The term covers both OTA provisioning and provisioning by means of, e.g., smart cards. A WAP client may, for example, be provisioned with connectivity and application information by pushing configuration parameters over the air from a server to a WAP client. This specification defines the content encoding by what configuration parameters are presented to the WAP client in the provisioning framework. The content encoding is defined in terms of binary XML [WBXML] and is interpreted and handled at the application level of the WAP architecture. However, the handling and use of provisioned information is outside the scope of this specification.

For an overview of the provisioning process architecture, please refer to the Provisioning Architecture Overview Specification, [PROVARCH].

2. References

2.1 Normative References

[3GPP23107] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; QoS Concept and Architecture (Release 1999)", (3G TS 23.107 V3.4.0 (2000-10)), URL: http://www.3gpp.org/

[3GPP24008] "3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile radio interface layer 3 specification; Core Network Protocols - Stage 3; (Release 1999)", (3G TS 24.008 V3.5.0 (2000-09)), URL: http://www.3gpp.org/

[CLIENTID] "WAP Client ID Specification", WAP Forum™, WAP-196-ClientID, URL: http://www.openmobilealliance.org/

[CREQ] "Specification of WAP Conformance Requirements", WAP Forum™, WAP-221-CREQ, URL: http://www.openmobilealliance.org/

[E212] "ITU-T E.212 Identification Plan For Land Mobile Stations", ITU, URL: http://www.itu.org/

[E2ESEC] "WAP Transport Layer E2E Security Specification", WAP Forum™, WAP-187-TransportE2Esec, URL: http://www.openmobilealliance.org/

[GENFORM] "WAP General Formats Document", WAP Forum™, WAP-188-WAPGenFormats, URL: http://www.openmobilealliance.org/

[IANA] "Internet Assigned Numbers Authority", URL: http://www.iana.org/

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1, URL:http://www.openmobilealliance.org/

[IS683B] "Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems", TIA/EIA-683-B

[OBEX] "IrDA Object Exchange Protocol (OBEX™)", version 1.2, Infrared Data Association, URL: http://www.irda.org/

[PROVBOOT] "Provisioning Bootstrap 1.1", Open Mobile Alliance™, OMA-WAP-PROVBOOT-V1_1, URL: http://www.openmobilealliance.org/

[PROVUAB] "Provisioning User Agent Behaviour 1.1", Open Mobile Alliance™, OMA-WAP-PROVUAB-V1_1, URL: http://www.openmobilealliance.org/

[PUSHOTA] "WAP Push OTA Specification", WAP Forum™, WAP-235-PushOTA, URL: http://www.openmobilealliance.org/

[RFC791] "Internet Protocol", Postel, J., September 1981, URL: http://www.ietf.org/rfc/rfc791.txt

[RFC2045] "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", N. Freed, N. Borenstein, November 1996, URL: http://www.ietf.org/rfc/rfc2045.txt

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997. URL: http://www.ietf.org/rfc/rfc2119.txt

[RFC2234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. November 1997. URL: http://www.ietf.org/rfc/rfc2234.txt

[RFC2279] "UTF-8, a transformation format of ISO 10646", ed. F. Yergeau, 1998, URL: http://www.ietf.org/rfc/rfc2279.txt

[RFC2373] "IP Version 6 Addressing Architecture", Hinden, R and S. Deering, July 1998, URL: http://www.ietf.org/rfc/rfc2373.txt

[RFC2396] "Uniform Resource Identifiers (URI): Generic Syntax", T.Berners-Lee, et al., August 1998, URL: http://www.ietf.org/rfc/rfc2396.txt

[RFC2617] "HTTP Authentication: Basic and Digest Access Authentication", J. Franks, et al., June 1999,

URL: http://www.ietf.org/rfc/rfc2617.txt.

[TIA/EIA-136-005A] "Introduction, Identity, and Semi-Permanent Memory", TIA/EIA

[WAPWDP] "Wireless Datagram Protocol Specification", WAP Forum™, WAP-259-WDP, URL: http://www.openmobilealliance.org/

[WBXML] "WAP Binary XML Content Format", WAP Forum™, WAP-192-WBXML, URL: http://www.openmobilealliance.org/

[WINA] "WAP Interim Naming Authority", Open Mobile Alliance™, URL: http://www.wapforum.org/wina/

[XML] "Extensible Markup Language (XML) 1.0 (Second edition)", W3C Recommendation 6 October 2000, REC-xml-20001006, URL: http://www.w3.org/TR/2000/REC-xml-20001006

[3GPP23107] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; QoS Concept and Architecture (Release 1999)", (3G TS 23.107 V3.4.0 (2000-10)), URL: http://www.3gpp.org/

[OMNA] Open Mobile Naming Authority, URL: http://www.openmobilealliance.org/tech/omna

2.2 Informative References

[MD5] "The MD5 Message-Digest Algorithm", RFC 1321, MIT Laboratory for Computer Science, RSA Data Security Inc., April 1992.

[PROVARCH] "Provisioning Architecture Overview 1.1", Open Mobile Alliance™, OMA-WAP-PROVARCH-V1_1, URL: http://www.openmobilealliance.org/

[PROVSC] "Provisioning Smart Card 1.1", Open Mobile Alliance™, OMA-WAP-PROVSC-V1_1, URL: http://www.openmobilealliance.org/

[WAPARCH] "WAP Architecture". WAP Forum™. WAP-210-WAPArch, URL: http://www.openmobilealliance.org/

[WDNS] "Wireless Profiled DNS Specification", Open Mobile Alliance™, OMA-WAP-DNS-1_0, URL: http://www.openmobilealliance.org/

[WINAProcess] "WAP WINA Process Document", WAP-212-WINAProcess, WAP Forum™, URL: http://www.wapforum.org/wina/

[WSP] "Wireless Session Protocol Specification", Open Mobile Alliance™, OMA-WAP-WSP-1_0, URL: 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.

3.2 Definitions

Application Server Access Point	An addressable entity through which the services of a specific application instance are available when it is accessed using one or more application protocols. The realisation of an application service access point may be a single process running on a single server, but it may also be composed of multiple processes or distributed across multiple physical servers with distinct network addresses. For instance, an 'e-mail server' might use a single computer to handle outgoing SMTP queues and implement mailbox access with several computers across which the mailbox storage is distributed.
Characteristics	This document uses the term characteristics to define the characteristics of, typically, a Network Element (access point, proxy). The word is broad enough to be used in all the required contexts.
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.
Default Proxy	The default proxy, or home proxy, defines the preferred proxy of the configuration context. The preferred proxy is defined by the largest domain scope, and in case of conflict, is defined by the highest priority. Priority is defined as a function of order of discovery.
Domain Description	The navigation and configuration information defines addresses and access parameters to connect to proxies. Each proxy can serve one or more domains. The DOMAIN can be a partial URL, expressing wildcard characteristics. www.service.com/protected/ www.service.com/ .service.com/ The DOMAIN of the proxy is defined as a parameter of the proxy characteristic.
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.
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.
Provisioning document	A particular instance of an XML document encoded according to the provisioning content specification [PROVCONT].
Proxy Navigation Mechanism	An in-band mechanism to provision the device in real time as defined in [E2ESEC].
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 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.
WAP Proxy	The WAP proxy is an endpoint for the WTP, WSP and WTLS protocols, as well as a proxy that is able to access WAP content. A WAP Proxy can have functionality such as that of, for example, a WSP Proxy or a WTA Proxy.
WSP Proxy	A generic WAP proxy, similar in functionality to a HTTP proxy. It is a variant of a WAP Proxy.
WTA Proxy	The WTA Proxy is a Wireless Telephony proxy as defined by WAP.

3.3 Abbreviations

AAA	Authentication, Authorization, and Accounting
APN	Access Point Name
CDMA	Code Division Multiple Access
CDPD	Cellular Digital Packet Data
CHAP	Challenge Handshake Authentication Protocol
CSD	Circuit Switched Data
DNS	Domain Name System
DTD	Document Type Definition
GHOST	GSM Hosted SMS Teleservice
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GUTS	General UDP Transport Service
HA	Home Agent
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
ITSI	Individual TETRA Subscriber Identity
MAN	Mobitex Subscription Number
ME	Mobile Equipment
MIME	Multipurpose Internet Mail Extensions
MMS	Multimedia Messaging Service
NAP	Network Access Point
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority
OTA	Over The Air
PAP	Password Authentication Protocol
PDP	Packet Data Protocol
RAS	Remote Access Server
SDS	Short Data Service
SID	System Identity

SIM	Subscriber Identity Module
SME	Short Message Entity
SMS	Short Message Service
SMSC	Short Message Service Centre
SOC	System Operator Code
SPI	Security Parameter Index
TETRA	Terrestrial Trunked Radio
TPS	Trusted Provisioning Server
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
USSD	Unstructured Supplementary Service Data
USSDC	Unstructured Supplementary Service Data Centre
WAP	Wireless Application Protocol
WBXML	WAP Binary XML
WSP	Wireless Session Protocol
WTA	Wireless Telephony Application
WTLS	Wireless Transport Layer Security
WTLS-SS	WTLS Shared Secret
WTP	Wireless Transaction Protocol
XML	Extensible Mark-up Language

4. Architectural Overview

Provisioning documents are binary encoded XML documents [WBXML] with a special MIME type that is interpreted at the application level on the ME. The handling and use of the provisioned information is outside the scope of this specification.

The XML DTD defines two elements; a CHARACTERISTIC element and a PARM element. The PARM element is used to provide values for the individual parameters, while the CHARACTERISTIC element is used to group parameters into logical entities that are related to a specific characteristic of the configuration space. Section 4.1 defines the XML DTD.

The configuration space may be defined in terms of the following main characteristics: Parameters related to logical proxies, parameters related to physical proxies, parameters related to network access points (NAPs), parameters related to the bootstrap process, parameters related to (ME) vendor specific configuration, parameters related to Client Identity, parameters related to applications, and parameters related to access rules. Additional characteristics may easily be added later by defining new characteristic types and parameter names. ME implementations MUST be designed with this in mind. An overview of the data model is presented in section 4.2.

Provisioning has been defined so that each provisioning document must be complete in the sense that information provided in one document cannot rely explicitly on information provided in another document. For example, if a physical proxy is to be used with a specific NAP, this NAP must be defined in the same provisioning document. Implicit reference to information defined in other documents is allowed. This is, for example, the case when using the INTERNET as a value for the TO-NAPID parameter, which means that reference is made to an arbitrary NAP definition that has an INTERNET parameter specified.

Logical proxies (the PXLOGICAL characteristic) have a number of physical instances, i.e. physical proxies (the PXPHYSICAL characteristic). Each logical proxy has a name, a unique ID, a startpage URL, and some parameters like port number values that are shared between all physical instances of the logical proxy.

Each proxy may serve one or several URL domains. Proxies may also vary in the protocols and services they support. To this end, PORT characteristics may be provided so that bindings between port numbers and protocols or services can be defined for each proxy.

The physical proxies refer to a number of NAP definitions (the NAPDEF characteristic), which can be used with the physical proxy in question. A NAPDEF characteristic has to supply definitions for all the parameters that are relevant to a particular NAP.

In the sections to follow, each of the characteristics and their associated parameters will be described along with the restrictions that apply to the occurrence and values of the parameters.

4.1 Provisioning Reference Information

Provisioning is an application of [XML] version 1.0. An implementation conforming to this specification MUST support the WAP-PROVISIONINGDOC DTD defined in this chapter.

4.1.1 Document Identifiers

4.1.1.1 SGML Public Identifier

-//WAPFORUM//DTD PROV 1.0//EN

4.1.1.2 Connectivity Media Type

Textual form:

```
text/vnd.wap.connectivity-xml
```

Tokenized form:

```
application/vnd.wap.connectivity-wbxml
```

4.1.2 Document Type Definition

The provisioning document format is based on a very simple XML DTD:

```
<!--
Provisioning Document Type Definition
Provisioning is an XML language. Typical Usage:

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


<!ELEMENT wap-provisioningdoc (characteristic+)>
<!ATTLIST wap-provisioningdoc
  version   CDATA #IMPLIED
>

<!ELEMENT characteristic (parm*, characteristic*)>
<!ATTLIST characteristic
  type CDATA #REQUIRED
>

<!ELEMENT parm EMPTY>
<!ATTLIST parm
  name  CDATA #REQUIRED
  value CDATA #IMPLIED
>
```

4.2 Overview of Data Model

The above XML DTD provides a flexible and extensible framework for parsing configuration parameters by means of PARM elements grouped by CHARACTERISTIC elements. The description of each of the possible PARM values and CHARACTERISTIC types is given in the following sections, while a short structural overview of the data model is given here.

The notation is such that **bold underlines** indicates parameters used for links, *italic* indicates parameters affected by external events, plus (+) indicates that the parameter can occur 1 or more times, star (*) indicates that the parameter can occur 0 or more times, question mark (?) indicates that the parameter can occur 0 or 1 times, empty ( ) indicates that the parameter is required within the scope of the encapsulating characteristic and that it can occur only once.

```
characteristic : PXLOGICAL *
{
    parm: PROXY-ID
    parm: PROXY-PW ?
    parm: PPGAUTH-TYPE ?
    parm: PROXY-PROVIDER-ID ?
    parm: NAME
```

```
    parm: DOMAIN *
    parm: TRUST ?
    parm: MASTER ?
    parm: STARTPAGE ?
    parm: BASAUTH-ID ?
    parm: BASAUTH-PW ?
    parm: WSP-VERSION ?
    parm: PUSHENABLED ?
    parm: PULLENABLED ?

    characteristic: PXAUTHINFO *
    {
        parm: PXAUTH-TYPE
        parm: PXAUTH-ID ?
        parm: PXAUTH-PW ?
    }

    characteristic: PORT *
    {
        parm: PORTNBR
        parm: SERVICE *
    }

    characteristic: PXPHYSICAL +
    {
        parm: PHYSICAL-PROXY-ID
        parm: DOMAIN *
        parm: PXADDR
        parm: PXADDRTYPE ?
        parm: PXADDR-FQDN ?
        parm: WSP-VERSION ?
        parm: PUSHENABLED ?
        parm: PULLENABLED ?
        parm: TO-NAPID +

        characteristic: PORT *
        {
            parm: PORTNBR
            parm: SERVICE *
        }
    }
}

characteristic: NAPDEF *
{
    parm: NAPID
    parm: BEARER *
    parm: NAME
    parm: INTERNET ?
    parm: NAP-ADDRESS
    parm: NAP-ADDRTYPE ?
    parm: DNS-ADDR *
    parm: CALLTYPE ?
    parm: LOCAL-ADDR ?
    parm: LOCAL-ADDRTYPE ?
    parm: LINKSPEED ?
```

```
    parm: DNLINKSPEED ?
    parm: LINGER ?
    parm: DELIVERY-ERR-SDU ?
    parm: DELIVERY-ORDER ?
    parm: TRAFFIC-CLASS ?
    parm: MAX-SDU-SIZE ?
    parm: MAX-BITRATE-UPLINK ?
    parm: MAX-BITRATE-DNLINK ?
    parm: RESIDUAL-BER ?
    parm: SDU-ERROR-RATIO ?
    parm: TRAFFIC-HANDL-PRIO ?
    parm: TRANSFER-DELAY ?
    parm: GUARANTEED-BITRATE-UPLINK ?
    parm: GUARANTEED-BITRATE-DNLINK ?
    parm: MAX-NUM-RETRY ?
    parm: FIRST-RETRY-TIMEOUT ?
    parm: REREG-THRESHOLD ?
    parm: T-BIT ?

    characteristic: NAPAUTHINFO *
    {
        parm: AUTHTYPE
        parm: AUTHNAME ?
        parm: AUTHSECRET ?
        parm: AUTH-ENTITY *
        parm: SPI ?
    }

    characteristic: VALIDITY *
    {
        parm: COUNTRY ?
        parm: NETWORK ?
        parm: SID ?
        parm: SOC ?
        parm: VALIDUNTIL ?
    }
}

characteristic: BOOTSTRAP *
{
    parm: NAME ?
    parm: NETWORK *
    parm: COUNTRY ?
    parm: PROXY-ID *
    parm: PROVURL ?
    parm: CONTEXT-ALLOW ?
}

characteristic : CLIENTIDENTITY ?
{
    parm: CLIENT-ID
}

characteristic: VENDORCONFIG *
{
    parm: NAME
    parm: *
}
```

```
characteristic : APPLICATION *
{
    parm: APPID
    parm: PROVIDER-ID ?
    parm: NAME ?
    parm: AACCEPT ?
    parm: APROTOCOL ?
    parm: TO-PROXY *
    parm: TO-NAPID *
    parm: ADDR *

    characteristic : APPADDR *
    {
        parm: ADDR
        parm: ADDRTYPE ?

        characteristic: PORT *
        {
            parm: PORTNBR
            parm: SERVICE *
        }
    }
    characteristic : APPAUTH *
    {
        parm: AAUTHLEVEL ?
        parm: AAUTHTYPE ?
        parm: AAUTHNAME ?
        parm: AAUTHSECRET ?
        parm: AAUTHDATA ?
    }
    characteristic : RESOURCE *
    {
        parm: URI
        parm: NAME ?
        parm: AACCEPT ?
        parm: AAUTHTYPE ?
        parm: AAUTHNAME ?
        parm: AAUTHSECRET ?
        parm: AAUTHDATA ?
        parm: STARTPAGE ?
    }
}

characteristic : ACCESS *
{
    parm: RULE +
    parm: APPID *
    parm: PORTNBR *
    parm: DOMAIN *
    parm: TO-NAPID *
    parm: TO-PROXY *
}
```

4.3 Media Type Parameter

The connectivity media type may contain security information, which is transported as parameters to the media type *application/vnd.wap.connectivity-wbxml*. The security information consists of the message authentication code and the security method. The parameters MAC and SEC have been defined for this purpose and these MUST be supported by the WAP client.

Parameters

SEC

The parameter specifies the security mechanism used (if it is not present, no security is used). If present it MUST take one of the values USERPIN, USERPINMAC, NETWPIN, USERNETWPIN [PROVBOOT]. If the parameter MAC is provided, the parameter SEC MUST also be present.

The parameter SEC can have the following values:

Value	Meaning
0	NETWPIN
1	USERPIN
2	USERNETWPIN
3	USERPINMAC

MAC

This parameter contains an even number of (upper case) hexadecimal digits used to authenticate the sender of the document and ensure integrity of the document. Quote characters MUST NOT be placed around the parameter value. The calculation of the MAC is defined in other provisioning specifications, such as the "WAP Provisioning Bootstrap Specification" [PROVBOOT].

4.4 The WAP-PROVISIONINGDOC element

This element encapsulates all the provisioned information. It has the following attribute:

Attribute

version

An optional attribute that contains version information. The version for the current specification is the string "1.1". An ME MUST only use documents that either do not have this attribute or have a version number which matches the major version number of the provisioning content type that the ME understands.

Increase of the minor version number indicates that the changes introduced are backward compatible with the

previous version(s), whereas increase of the major version number indicates introduction of non-backward compatible changes.

4.5 The CHARACTERISTIC element

This element is used to group the provisioned information into logical units. It has a required type attribute, which can take on the following values:

Attributes

type

PXLOGICAL, PXPHYSICAL, PXAUTHINFO, PORT, NAPDEF, NAPAUTHINFO, VALIDITY, BOOTSTRAP, CLIENTIDENTITY, VENDORCONFIG, APPLICATION, APPADDR, APPAUTH, RESOURCE, ACCESS.

A characteristic of a particular type can only accept certain parameters, and parameters defined in one characteristic can generally not be overwritten by another.

Value	Meaning
PXLOGICAL	Definition of a logical proxy
PXPHYSICAL	Definition of a physical proxy
PXAUTHINFO	Definition of authentication information within a logical proxy
PORT	Defines port bindings
NAPDEF	Definition of a Network Access Point
NAPAUTHINFO	Definition of authentication information within a network access point
VALIDITY	Defines country, network, and/or period of time where a certain NAPDEF is valid
BOOTSTRAP	Defines parameters relevant for bootstrapping
CLIENTIDENTITY	Defines the client-ID
VENDORCONFIG	Vendor specific configuration
APPLICATION	Definition of general application specific parameters
APPADDR	Definition of application address information
APPAUTH	Definition of application authentication information
RESOURCE	Definition of resources within an application
ACCESS	Definition of a set of access rules for the terminal

4.5.1 Characteristics of type PXLOGICAL

PXLOGICAL characteristics define logical proxies and may only occur at the root of a provisioning document. This characteristic MUST be supported by the WAP client.

4.5.2 Characteristics of type PXPHYSICAL

PXPHYSICAL characteristics convey information on physical instances of a logical proxy and should be listed according to priority inside a PXLOGICAL characteristic. The ME MAY choose to rely on the so defined priority to select a physical proxy. The ME MAY reuse WTLS sessions with all PXPHYSICAL defined in the scope of a single PXLOGICAL. For WSP sessions, on the other hand, the ME MAY use the suspend/resume functionality to move sessions between any of these physical proxies. This characteristic MUST be supported by the WAP client.

4.5.3 Characteristics of type PXAUTHINFO

PXAUTHINFO characteristics define the binding between a proxy authentication method and its corresponding authentication parameters. It may only occur within a PXLOGICAL characteristic.

4.5.4 Characteristics of type PORT

PORT characteristics define the binding between a port number and one or more protocols or services. It may only occur in PXLOGICAL, PXPHYSICAL, and APPADDR characteristics. This characteristic MUST be supported by the WAP client.

4.5.5 Characteristics of type NAPDEF

NAPDEF characteristics define network access points and may only occur at the root of a provisioning document. This characteristic MUST be supported by the WAP client.

4.5.6 Characteristics of type NAPAUTHINFO

NAPAUTHINFO characteristics define the binding between an authentication method and its corresponding authentication parameters. It may only occur at the root of a NAPDEF characteristic.

4.5.7 Characteristics of type VALIDITY

The VALIDITY characteristic indicates the range (in time as well as in terms of country and network codes) where a certain NAPDEF is valid. It may only occur at the root of a NAPDEF characteristic.

4.5.8 Characteristics of type BOOTSTRAP

The BOOTSTRAP characteristic is used to define parameters of use during the bootstrap process. This characteristic may only occur at the root of the provisioning document.

4.5.9 Characteristics of type CLIENTIDENTITY

CLIENTIDENTITY characteristics define a global identity. It may only occur at the root of a provisioning document.

4.5.10 Characteristics of type VENDORCONFIG

The VENDORCONFIG characteristic is used for (ME) vendor specific provisioning. It may only occur at the root of a provisioning document.

4.5.11 Characteristics of type APPLICATION

The APPLICATION characteristic is used to define application protocol parameters and to describe the attributes of an application service access point available using the protocol. This characteristic may only occur at the root of the provisioning document.

Characteristics of type APPADDR

The APPADDR characteristic is used to define address parameters for an application protocol. This characteristic may only occur within the APPLICATION characteristic.

4.5.12 Characteristics of type APPAUTH

The APPAUTH characteristic is used to specify authentication parameters related to an APPLICATION characteristic. This characteristic may only occur within the APPLICATION characteristic.

4.5.13 Characteristics of type RESOURCE

The RESOURCE characteristic is used to describe the resources available at an application service access point and access parameters related to them. This characteristic may only occur within the APPLICATION characteristic.

4.5.14 Characteristics of type ACCESS

The ACCESS characteristic defines a set of access rules that the terminal MUST obey and may only occur at the root of the provisioning document. This characteristic MUST be supported by the WAP client.

4.6 The PARM element

The PARM element is a general purpose slot for various parameters of each characteristic. The attribute NAME of the element defines the usage of the element.

A parameter with a type that does not add value can be omitted from the definition. For example, if proxy authentication is not performed then the parameter PXAUTH-TYPE can be omitted, and subsequently the parameters PXAUTH-ID and PXAUTH-PW can also be omitted. Some parameters, like the DOMAIN parameter, can be used multiple times within the characteristic.

The PARM element MAY be used for providing provisioning parameters specific to an application service or application protocol. However, these SHOULD be registered with WINA [WINA] to guarantee interoperability. The details on how the parameters defined in this specification are used SHOULD be registered with WINA, too. The needed registration information is detailed in the WINA Process Document [WINAProcess] section covering "WPG Client Provisioning".

Attributes

name

The NAME of the parameter. Permitted values depend on the type of characteristics the PARM element is a sub-element of.

value

The VALUE of the parameter. Permitted values depend on the NAME attribute of the element.

4.6.1 Parameters for PXLOGICAL characteristics

The PXLOGICAL characteristic indicates the name and parameters needed to access a particular logical WAP Proxy from the wireless terminal. The PXLOGICAL characteristic is linked to a NAPDEF element to provide all the necessary access information. Note that the parameters listed below are described in the scope of this particular characteristic.

Names and values of parameters

PROXY-ID

The PROXY-ID is used to define one logical WAP proxy entity. It is also used to link a proxy to session and security contexts. A PROXY-ID MUST be globally unique. Uniqueness MUST be obtained by either using a fully qualified Internet domain name (i.e. hostname as defined in section 3.2.2 of [RFC2396]) or a globally unique IP address (IPv4 [RFC791] in decimal format with dots as delimiters or IPv6 [RFC2373], as hexadecimal numbers with colons as delimiters or as a combination of hexadecimal and decimal numbers with dots and colons as delimiters). This parameter MUST be supported by the WAP client.

PROXY-PW (0 or 1 entries)

The PROXY-PW indicates the authentication password for the proxy. PROXY-ID and PROXY-PW are used as authentication parameters for push proxy authentication to the client. This parameter MUST be supported if the client supports OTA-HTTP [PushOTA] services.

PPGAUTH-TYPE (0 or 1 entries)

The PPGAUTH-TYPE parameter links the PROXY-ID and PROXY-PW to an authentication method. Possible values are "HTTP-BASIC" and "HTTP-DIGEST" [PushOTA]. This parameter MUST be supported if the client supports OTA-HTTP services.

PROXY-PROVIDER-ID (0 or 1 entries)

The PROXY-PROVIDER-ID is used to verify the identity of a proxy when using certificate based server authentication. If server certificate authentication is used, and the PROXY-PROVIDER-ID has been defined, then service credentials of the certificate MUST match the PROXY-PROVIDER-ID. The format MUST be either a fully qualified Internet domain name (i.e. hostname as defined in section 3.2.2 of [RFC2396]) or a globally unique IP address (IPv4 [RFC791] in decimal format with dots as delimiters or IPv6 [RFC2373], as hexadecimal numbers with colons as delimiters or as a combination of hexadecimal and decimal numbers with dots and colons as delimiters).

NAME

The NAME indicates a logical, user readable, identity (property) of the configuration element. This parameter MUST be supported by the WAP client.

DOMAIN (0 to 4 entries)

The DOMAIN parameter indicates a domain, for which the proxy is responsible. The proxy might support multiple domains. The DOMAIN parameter MUST be either in the syntax described in [PROVUAB] or an absolute URI [RFC2396]. If the DOMAIN parameter contains an IPv4-address, it MUST be given in decimal format with dots as delimiters as defined in [RFC2396]. If the DOMAIN parameter contains an IPv6-address [RFC2373], it MUST be given as hexadecimal numbers with colons as delimiters or as a combination of hexadecimal and decimal numbers with dots and colons as delimiters. If the DOMAIN parameter is missing, this MUST be interpreted as if an empty value was given. This parameter MUST be supported by the WAP client.

TRUST (0 or 1 entries)

The TRUST can be used to define that a particular proxy is trusted. For example, provisioning information received from the trusted proxy can be accepted. Note that it is possible that the user does not have a trusted proxy. The trusted proxy does not have to be the home (default) proxy. The parameter does not take a value.

MASTER (0 or 1 entries)

The MASTER is used to define that a particular proxy is allowed to send navigation documents to the device, using the Proxy Navigation Mechanism defined in [E2ESEC]. The parameter does not take a value.

STARTPAGE (0 or 1 entries)

The STARTPAGE parameter MUST be an absolute URI [RFC2396] and defines the homepage or start page associated with the services accessible from the proxy. The STARTPAGE MAY be used to provide different services to different users. If the scheme is missing from the STARTPAGE parameter, then "http" is assumed. This parameter MUST be supported by the WAP client.

BASAUTH-ID (0 or 1 entries)

The BASAUTH-ID indicates the basic authentication identifier for the startpage. This parameter MUST be supported by the WAP client.

BASAUTH-PW (0 or 1 entries)

The BASAUTH-PW indicates the basic authentication password for the startpage. This parameter MUST be supported by the WAP client.

WSP-VERSION (0 or 1 entries)

The WSP-VERSION indicates the WSP encoding version that the proxy in question supports. The format of this parameter is an integer representing the major version number followed by a "." and an integer representing the minor version number. If the parameter is not present or if no value is given, then the default value 1.2 should be assumed.

PUSHENABLED (0 or 1 entries)

This parameter takes one of the values 0 or 1. If the value is 1 for a given logical proxy, this proxy will support push. The ME is consequently advised to enable push. If the value is 0 for a given logical proxy, this proxy will not support push. If the parameter is not present or if no value is given, then the default value 0 should be assumed. The parameter is advisory only and an ME might override the recommendation. In particular, it MUST be ignored if a SERVICE associated with the proxy always supports push.

PULLENABLED (0 or 1 entries)

This parameter takes one of the values 0 or 1. If the value is 1 for a given logical proxy, this proxy will support pull. If the value is 0 for a given logical proxy, this proxy will not support pull. If the parameter is not present or if no value is given, then the default value 1 should be assumed. The parameter is advisory only and an ME might override the recommendation. In particular, it MUST be ignored, if a SERVICE associated with the proxy always supports pull.

4.6.2 Parameters for PXPHYSICAL characteristics

The PXPHYSICAL characteristic is only allowed to be used within the characteristic of a logical PROXY. Note that the parameters listed below are described in the scope of this particular characteristic.

Names and values of parameters

PHYSICAL-PROXY-ID

The PHYSICAL-PROXY-ID is used to define one physical WAP proxy entity. The PHYSICAL-PROXY-ID MUST be unique within its enclosed structure, i.e. within the PXLOGICAL characteristic. This parameter MUST be supported by the WAP client.

DOMAIN (0 to 4 entries)

The DOMAIN parameter indicates a domain, for which the proxy is responsible. The proxy might support multiple domains. The DOMAIN parameter MUST be either in the syntax described in [PROVUAB] or an absolute URI [RFC2396]. If the DOMAIN parameter contains an IPv4-address, it MUST be given in decimal format with dots as delimiters as defined in [RFC2396]. If the DOMAIN parameter contains an IPv6-address [RFC2373], it MUST be given as hexadecimal numbers with colons as delimiters or as a combination of hexadecimal and decimal numbers with dots and colons as delimiters.

The domain definition must be interpreted as a subset of all the URI defined by the domain parameter of PXLOGICAL. The DOMAIN is used to select the physical instance of the logical proxy, and thus for example bearer and network access point. If no DOMAIN parameter is supplied for a physical proxy definition, the corresponding parameter value from the logical proxy definition is assumed to apply for the physical proxy as well.

PXADDR

The PXADDR can store addresses of different kinds, for example an IP address or a SME number. The type of address in the field is defined by the PXADDRTYPE parameter. This parameter MUST be supported by the WAP client.

PXADDRTYPE	Content of PXADDR
IPV4	An IPv4 address [RFC791] represented in decimal format with dots as delimiters
IPV6	An IPv6 address [RFC2373] represented as hexadecimal numbers with colons as delimiters or as a combination of hexadecimal and decimal numbers with dots and colons as delimiters
E164	A phone number according to the E164 scheme [GENFORM]
ALPHA	Generic alphanumeric address (as defined by alphanum in [RFC2396])

PXADDRTYPE (0 or 1 entries)

The PXADDRTYPE indicates the format and the interpretation of the PXADDR attribute. The PXADDRTYPE can indicate an IP address, a phone number according to the E164 scheme, or a generic alphanumeric address format. If the parameter is not present or if no value is given, the default value IPV4 should be assumed. This parameter MUST be supported by the WAP client.

Value
IPV4 (default)
IPV6
E164
ALPHA

PXADDR-FQDN (0 or 1 entries)

The PXADDR-FQDN parameter can store a proxy address given as a fully qualified domain name. A PXADDR-FQDN MUST be a fully qualified Internet domain name (i.e. hostname as defined in section 3.2.2 of [RFC2396]).

WSP-VERSION (0 or 1 entries)

The WSP-VERSION indicates the WSP encoding version that the proxy in question supports. The format of this parameter is an integer representing the major version number followed by a "." and an integer representing the minor version number. If no WSP-VERSION parameter is supplied for a physical proxy definition, the corresponding parameter value from the logical proxy definition is assumed to apply for the physical proxy as well.

PUSHENABLED (0 or 1 entries)

This parameter takes one of the values 0 or 1. If the value is 1 for a given physical proxy, this physical proxy will support push. The ME is consequently advised to enable push. If the value is 0 for a given physical proxy, this proxy will not support push. If no PUSHENABLED parameter is supplied for a physical proxy definition, the corresponding parameter value from the logical proxy definition is assumed to apply for the physical proxy as well. The parameter is advisory only and an ME might override the recommendation. In particular, it MUST be ignored if a SERVICE associated with the proxy always supports push.

PULLENABLED (0 or 1 entries)

This parameter takes one of the values 0 or 1. If the value is 1 for a given physical proxy, this physical proxy will support pull. If the value is 0 for a given physical proxy, this proxy will not support pull. If no PULLENABLED parameter is supplied for a physical proxy definition, the corresponding parameter value from the logical proxy definition is assumed to apply for the physical proxy as well. The parameter is advisory only and an ME might override the recommendation. In particular, it MUST be ignored, if a SERVICE associated with the proxy always supports pull.

TO-NAPID (1 or more entries)

This parameter refers to a network access point with a matching NAPID parameter. It is only possible to refer to network access points defined within the same provisioning document (except if the INTERNET attribute is set in the NAPDEF). Several TO-NAPID parameters may be listed for a given physical proxy. The order of the list indicates the priority of the individual network access points. However, client preferences MAY also be considered which might affect the priority order (see also [PROVUAB]). One TO-NAPID has a special predefined meaning. If the TO-NAPID is INTERNET, it implies that the ME can select any network access point with the attribute INTERNET defined. This parameter MUST be supported by the WAP client.

4.6.3 Parameters for PXAUTHINFO characteristics

The PXAUTHINFO characteristic is only allowed to be used within a PXLOGICAL characteristic. Note that the parameters listed below are described in the scope of this particular characteristic.

PXAUTH-TYPE

The PXAUTH-TYPE indicates the proxy authentication method: HTTP proxy authentication or WTLS methods. Possible values are "HTTP-BASIC", "HTTP-DIGEST" and "WTLS-SS". This parameter does not indicate the actual authentication method to use when connecting to the proxy, but links the authentication parameters PXAUTH-ID and PXAUTH-PW to an authentication method. The PXAUTH-TYPE MUST be unique within its enclosed structure, i.e. within the PXLOGICAL characteristic.

PXAUTH-ID (0 or 1 entries)

The PXAUTH-ID indicates the proxy authentication identifier. If it is missing then the global id of the device should be used (see [ProvUAB] section 4.7). The global identifier can be defined for example using the CLIENTIDENTITY characteristic.

PXAUTH-PW (0 or 1 entries)

The PXAUTH-PW indicates the proxy authentication secret. The usage of the parameter is defined by the PXAUTH-TYPE.

4.6.4 Parameters for PORT characteristics

The PORT characteristic is only allowed to be used within PXLOGICAL,PXPHYSICAL, or APPADDR characteristics. Note that the parameters listed below are described in the scope of this particular characteristic.

Names and values of parameters

PORTNBR

The PORTNBR parameter contains the value of the port number. The port number must be given as a decimal number and must fit within the range of a 16 bit unsigned integer. The PORTNBR MUST be unique within its enclosed structure, i.e. within the PXLOGICAL, PXPHYSICAL, or APPADDR characteristic.

If the port number is well known [WAPWDP] [IANA], then the service behind the port is implied and the parameter SERVICE MAY be omitted. If the port number is not well known, then no service is implied and the service behind the port is defined in parameter SERVICE. If the port number is not well known and the parameter SERVICE is omitted, then the ME MUST assume a service according to its preferences.

If the parameter SERVICE is present, then the definition in the SERVICE parameter overrides the implicit meaning.

This parameter MUST be supported by the WAP client.

SERVICE (0 or more entries)

The SERVICE parameter specifies which service is available behind this particular port number. Possible values are defined in the table below. The service can also be indicated by a well known port number being given as SERVICE. The format of this port number is as defined in PORTNBR. This parameter MUST be supported by the WAP client.

Service	Explanation
CL-WSP	WAP connection-less session service
CO-WSP	WAP session service
CL-SEC-WSP	WAP secure connection-less session service
CO-SEC-WSP	WAP secure session service
CO-SEC-WTA	WAP WTA secure session service (over WSP)
CL-SEC-WTA	WAP WTA secure connection-less session service (over WSP)
OTA-HTTP-TO	OTA-HTTP service (push), TO-TCP [PushOTA]
OTA-HTTP-TLS-TO	OTA-HTTP secure service (push), TO-TCP [PushOTA]
OTA-HTTP-PO	OTA-HTTP service (push), PO-TCP [PushOTA]
OTA-HTTP-TLS-PO	OTA-HTTP secure service (push), PO-TCP [PushOTA]

4.6.5 Parameters for NAPDEF characteristics

This section defines permitted parameters for the NAPDEF type of the characteristic, i.e. the names and parameters needed to access the backbone data network from the wireless terminal. Note that the parameters listed below are described in the scope of this particular characteristic.

Names and values of parameters

NAPID

The NAPID is used to link to the TO-NAPID parameter of the PXPHYSICAL characteristic. The NAPID MUST be unique within its enclosed structure, i.e. within the configuration context. This parameter MUST be supported by the WAP client.

BEARER (0 or more entries)

The BEARER indicates which network type (in addition to address type) the definition is valid for. This parameter MUST be supported by the WAP client.

Value
GSM-USSD
GSM-SMS
ANSI-136-GUTS
IS-95-CDMA-SMS
IS-95-CDMA-CSD
IS-95-CDMA-PACKET
ANSI-136-CSD
ANSI-136-GPRS
GSM-CSD
GSM-GPRS
AMPS-CDPD
PDC-CSD
PDC-PACKET
IDEN-SMS
IDEN-CSD
IDEN-PACKET
FLEX/REFLEX
PHS-SMS
PHS-CSD
TETRA-SDS
TETRA-PACKET
ANSI-136-GHOST
MOBITEX MPAK
CDMA2000-1X-SIMPLE-IP
CDMA2000-1X-MOBILE-IP

NAME

The NAME indicates a logical, user readable, identity (property) of the configuration element. In the NAPDEF element it typically indicates the "owner" of the RAS, and if the element is to be used while in the home network or while roaming. This parameter MUST be supported by the WAP client.

INTERNET (0 or 1 entries)

This parameter does not take any values. If it is present, it indicates that the network access point can be used to access proxies that are located on an IP-routable network segment, which is generic within the scope of the configuration context. The existence of the parameter does not imply that the IP routable network that can be accessed is similar in scope to the world wide Internet.

NAP-ADDRESS

Contains all the digits and pauses needed to communicate with a remote entity and is defined in [GENFORM]. The format and the content of the parameter depend on the bearer type. The NAP-ADDRESS might contain for example

- The phone number of an access router
- A calling card dialling sequence
- A GPRS APN, which is an indirect address that has to be resolved by a network specific DNS mechanism.
- An address of an SMSC, or any other message centre

The NAP-ADDRESS should be in international format whenever possible, for example using the "+" notation as in GSM.

The type of address in the NAP-ADDRESS field is defined by the NAP-ADDRTYPE parameter. This parameter MUST be supported by the WAP client.

NAP-ADDRTYPE	Content of NAP-ADDRESS
IPV4	An IPv4 address [RFC791] represented in decimal format with dots as delimiters
IPV6	An IPv6 address [RFC2373] represented as hexadecimal numbers with colons as delimiters or as a combination of hexadecimal and decimal numbers with dots and colons as delimiters
E164	A phone number according to the E164 scheme [GENFORM]
ALPHA	Generic alphanumeric address (as defined by alphanum in [RFC2396])
APN	A GPRS APN as defined in [GENFORM]
SCODE	A USSD service code as defined in [GENFORM]
TETRA-ITSI	A TETRA SDS address with digits in decimal format [WAPWDP]
MAN	A Mobitex MAN address with digits in decimal format [WAPWDP]

NAP-ADDRTYPE (0 or 1 entries)

The NAP-ADDRTYPE indicates the format of the address in the NAP-ADDRESS. This parameter MUST be supported by the WAP client.

Value
IPV4
IPV6
E164 (default)
ALPHA
APN
SCODE
TETRA-ITSI
MAN

CALLTYPE (0 or 1 entries)

Some bearers may support different types of calls or different protocols to be used for data exchange. The CALLTYPE parameter is used to define this protocol or call type. If the parameter is not present or if no value is given, the default value ANALOG-MODEM should be assumed.

Value
ANALOG-MODEM (default)
V.120
V.110
X.31
BIT-TRANSPARENT
DIRECT-ASYNCHRONOUS-DATA-SERVICE

LOCAL-ADDR (0 or 1 entries)

If this parameter is provided, it defines the local address of the WAP Client according to the format specified by the LOCAL-ADDRTYPE parameter.

The type of address in the LOCAL-ADDR field is defined by the LOCAL-ADDRTYPE parameter.

LOCAL-ADDRTYPE	Content of LOCAL-ADDR
IPV4	An IPv4 address [RFC791] represented in decimal format with dots as delimiters
IPV6	An IPv6 address [RFC2373] represented as hexadecimal numbers with colons as delimiters or as a combination of hexadecimal and decimal numbers with dots and colons as delimiters

LOCAL-ADDRTYPE (0 or 1 entries)

The LOCAL-ADDRTYPE indicates the format of the address in the LOCAL-ADDR parameter. If the parameter is not present or if no value is given, the default value IPV6 should be assumed.

Value
IPV4
IPV6 (default)

DNS-ADDR (0 or more entries)

The DNS-ADDR can store the address of a DNS server. If the client implements [WDNS] this parameter MUST be supported. If this parameter is supported, at least two entries MUST be supported.
The address format MUST conform to the following table. It is the responsibility of the client to distinguish between the two address types.

Address type	Format of DNS-ADDR
IPv4	An IPv4 address [RFC791] represented in decimal format with dots as delimiters
IPv6	An IPv6 address [RFC2373] represented as hexadecimal numbers with colons as delimiters or as a combination of hexadecimal and decimal numbers with dots and colons as delimiters

LINKSPEED (0 or 1 entries)

Defines the speed on the up-link channel and optionally the down-link channel for circuit switched bearers. Possible values are "autobauding" or a number (baud in decimal format).

DNLINKSPEED (0 or 1 entries)

Defines the speed on the down-link channel for circuit switched bearers. Possible values are "autobauding" or a number (baud in decimal format). If this parameter is missing or if the ME does not support different up- and down-link speeds, the value of the LINKSPEED parameter may be assumed to be effective for the down-link channel as well.

LINGER (0 or 1 entries)

The LINGER parameter is used to define how long a connection should be kept active without any traffic. The parameter value is a decimal value expressed in seconds.

DELIVERY-ERR-SDU (0 or 1 entries)

The DELIVERY-ERR-SDU parameter indicates whether SDUs detected as erroneous shall be delivered or discarded. Values are defined in [3GPP24008] and are represented as hexadecimal numbers.

DELIVERY-ORDER (0 or 1 entries)

The DELIVERY-ORDER parameter indicates whether the PDP context bearer shall provide in-sequence SDU delivery or not. Values are defined in [3GPP24008] and are represented as hexadecimal numbers. Bits not part of the DELIVERY-ORDER parameter are set to zero, e.g. the value "with delivery order" is represented as 0x08.

TRAFFIC-CLASS (0 or 1 entries)

The TRAFFIC-CLASS defines the type of application for which the PDP context bearer service is optimised. For class descriptions see [3GPP23107] and values are defined in [3GPP24008]. The values are represented as hexadecimal numbers. Bits not part of the TRAFFIC-CLASS parameter are set to zero, e.g. the value "interactive class" is represented as 0x60.

MAX-SDU-SIZE (0 or 1 entries)

The MAX-SDU-SIZE parameter defines the maximum allowed SDU size and is used for admission control and policing. Values are defined in [3GPP24008] and are represented as hexadecimal numbers.

MAX-BITRATE-UPLINK (0 or 1 entries)

The MAX-BITRATE-UPLINK parameter defines the maximum number of bits delivered during a period of time in uplink. Values are defined in [3GPP24008] and are represented as hexadecimal numbers.

MAX-BITRATE-DNLINK (0 or 1 entries)

The MAX-BITRATE-DNLINK parameter defines the maximum number of bits delivered during a period of time in downlink. Values are defined in [3GPP24008] and are represented as hexadecimal numbers.

RESIDUAL-BER (0 or 1 entries)

The RESIDUAL-BER parameter indicates the undetected bit error ratio in the delivered SDUs. Values are defined in [3GPP24008] and are represented as hexadecimal numbers. Bits not part of the RESIDUAL-BER parameter are set to zero, e.g. the value "$1*10^{-5}$" is represented as 0x70.

SDU-ERROR-RATIO (0 or 1 entries)

The SDU-ERROR-RATIO parameter indicates the fraction of SDUs lost or detected as erroneous and is defined only for conforming traffic. Values are defined in [3GPP24008] and are represented as hexadecimal numbers.

TRAFFIC-HANDL-PRIO (0 or 1 entries)

The TRAFFIC-HANDL-PRIO parameter specifies the relative importance for handling of all SDUs belonging to the PDP context bearer compared to the SDUs of other bearers. Values are defined in [3GPP24008] and are represented as hexadecimal numbers.

TRANSFER-DELAY (0 or 1 entries)

The TRANSFER-DELAY parameter indicates the maximum delay for 95^{th} percentile of the distribution of delay for all delivered SDUs during the lifetime of a bearer service. Delay for an SDU is defined as the time from a request to transfer an SDU at one SAP to its delivery at the other SAP. Values are defined in [3GPP24008] and are represented as hexadecimal numbers. Bits not part of the TRANSFER-DELAY parameter are set to zero, e.g. the value "300 ms" is represented as 0x48.

GUARANTEED-BITRATE-UPLINK (0 or 1 entries)

The GUARANTEED-BITRATE-UPLINK parameter indicates the guaranteed number of bits delivered by the PDP context at a SAP within a period of time, divided by the duration of the period. Values are defined in [3GPP24008] and are represented as hexadecimal numbers.

GUARANTEED-BITRATE-DNLINK (0 or 1 entries)

The GUARANTEED-BITRATE-DNLINK parameter indicates the guaranteed number of bits delivered by the PDP context at a SAP within a period of time, divided by the duration of the period. Values are defined in [3GPP24008] and are represented as hexadecimal numbers.

MAX-NUM-RETRY (0 or 1 entries)

The MAX-NUM-RETRY parameter defines maximum Number of Retry for the MobileIP Registration. Values are represented as hexadecimal numbers. Valid values are 1-3. See [IS683B], section 3.5.8.6 for additional details. If the bearer value CDMA2000-1X-MOBILE-IP is supported then this parameter MUST be supported.

FIRST-RETRY-TIMEOUT (0 or 1 entries)

The FIRST-RETRY-TIMEOUT parameter defines the amount of time elapsed, in units of 250ms, between the first and second MobileIP Registration Requests, while the mobile station did not receive the MobileIP Registration Reply. Values are represented as hexadecimal numbers. Valid values are 1-7. See [IS683B], section 3.5.8.6 for additional details. If the bearer value CDMA2000-1X-MOBILE-IP is supported then this parameter MUST be supported.

REREG-THRESHOLD (0 or 1 entries)

The REREG-THRESHOLD parameter defines time, in units of minute, before the expiration of the registration lifetime that the mobile will try to reregister. Values are represented as hexadecimal numbers. Valid values are 1-63. See [IS683B], section 3.5.8.6 for additional details. If the bearer value CDMA2000-1X-MOBILE-IP is supported then this parameter MUST be supported.

T-BIT (0 or 1 entries)

The T-BIT parameter defines if reverse tunneling is required. There are no values for this parameter. Presence of the parameter indicates that reverse tunnelling is required. Parameter is omitted otherwise. See [IS683B], section 3.5.8.6 for additional details. If the bearer value CDMA2000-1X-MOBILE-IP is supported then this parameter MUST be supported.

4.6.6 Parameters for NAPAUTHINFO characteristics

The NAPAUTHINFO characteristic is only allowed to be used within a NAPDEF characteristic. Note that the parameters listed below are described in the scope of this particular characteristic.

AUTHTYPE

The AUTHTYPE is a parameter indicating the authentication protocol. Possible values are PAP, CHAP, and MD5. This parameter does not indicate the actual authentication method to use when connecting to the network access point, but links the authentication parameters AUTHNAME and AUTHSECRET to the authentication method. The AUTHTYPE MUST be unique within its enclosed structure, i.e. within the NAPDEF characteristic. If the bearer value CDMA2000-1X-MOBILE-IP is supported then the MD5 value MUST be supported.

AUTHNAME (0 or 1 entries)

The AUTHNAME parameter can contain the id (plaintext) needed to authenticate the user. This parameter is only needed if the AUTHTYPE parameter takes one of the values PAP or CHAP or MD5.

AUTHSECRET (0 or 1 entries)

The AUTHSECRET parameter can contain the password (plaintext) needed to authenticate the user. This parameter is only needed if the AUTHTYPE parameter takes one of the values PAP or CHAP or MD5.

AUTH-ENTITY (0 or more entries)

The parameter defines entity to which NAPAUTHINFO credentials are valid. Valid values are specified in the following table. If the bearer value CDMA2000-1X-MOBILE-IP is supported then the AUTH-ENTITY value MUST be supported. When the NAPAUTHINFO is valid for more than one entity, multiple instances of AUTH-ENTITY are specified.

Value	Description
AAA	Authentication credentials are valid for the AAA.
HA	Authentication credentials are valid for the HA.

SPI (0 or 1 entries)

The parameter defines whether Security Parameter Index is used between mobile and the AUTH-ENTITY – i.e. AAA or HA. The parameter is omitted if SPI is not used. See [IS683B], section 3.5.8.6 for additional details. If the bearer value CDMA2000-1X-MOBILE-IP is supported then the SPI value MUST be supported.

4.6.7 Parameters for VALIDITY characteristics

The VALIDITY element is used to define country code and network code parameters, or system identity and system operator code parameters, as well as the period of time in which a certain NAPDEF is valid. If NETWORK is defined, then COUNTRY MUST be present. If SID is defined, then SOC MUST be present. The VALIDITY characteristic is only allowed to be used within the characteristic of type NAPDEF. Note that the parameters listed below are described in the scope of this particular characteristic.

Names and values of parameters

COUNTRY (0 or 1 entries)

The COUNTRY indicates a Mobile Country Code as defined by ITU-T [E212]. The parameter is used to identify what resources to use when a mobile is in its home network or when the mobile is roaming. The COUNTRY MUST be unique within its enclosed structure, i.e. within the NAPDEF characteristic.

NETWORK (0 or 1 entries)

The NETWORK indicates a list of comma separated Mobile Network Codes in decimal format as defined by ITU-T [E212]. The parameter is used to identify what resources the mobile should use when it is registered to a particular network.

SID (0 or 1 entries)

The SID indicates a list of comma separated System IDs in decimal format as defined by [TIA/EIA-136-005A]. The parameter is used to identify what resources the mobile should use when it is registered to a particular network.

SOC (0 or 1 entries)

The SOC indicates a System Operator Code as defined by [TIA/EIA-136-005A]. The parameter is used to identify what resources the mobile should use when it is registered to a particular network. The SOC MUST be unique within its enclosed structure, i.e. within the NAPDEF characteristic.

VALIDUNTIL (0 or 1 entries)

Defines the end of the (time) period of validity. The parameter is expressed in seconds, from the time it is received by the client device.

4.6.8 Parameters for BOOTSTRAP characteristics

This section defines permitted parameters for the BOOTSTRAP characteristic. This characteristic is typically used within the bootstrap message. If NETWORK is defined, then COUNTRY MUST be present. Note that the parameters listed below are described in the scope of this particular characteristic.

If a provisioning document contains a PROVURL the PROVURL MUST be present only once in the provisioning document. The provisioning document may still contain multiple BOOTSTRAP characteristics but only one of them may contain a PROVURL. If the PROVURL is present in a BOOTSTRAP characteristic, NETWORK and COUNTRY MUST NOT be present in the same characteristic, since these are used to specify parameter settings for roaming purposes and the PROVURL is the unique identifier for the entire configuration context.

Names and values of parameters

NAME (0 or 1 entries)

The NAME indicates a logical, user readable, identity (property) of the configuration context.

NETWORK (0 or more entries)

The NETWORK parameter MUST contain a decimal value that indicates for which network code (as defined in ITU-T [E212]) the bootstrap information is valid.

COUNTRY (0 or 1 entries)

The COUNTRY parameter defines the Mobile Country Codes as defined by ITU-T [E212]. The parameter is used to identify which country code the bootstrap information is valid.

PROXY-ID (0 or more entries)

The PROXY-ID parameter contains the ID of a proxy that is available with this particular set of bootstrap information. It is only possible to refer to proxies defined within the same provisioning document.

PROVURL (0 or 1 entries)

The PROVURL MUST be an absolute URI [RFC2396] and defines the authority and path of the TPS. The path of a request can be extended, and still be within the scope of the TPS, but it cannot be shortened. The URL to be used to contact the Trusted Provisioning Server, for example, for requests for re-provisioning (roaming). The PROVURL MUST be globally unique and is the unique identifier of the configuration context. If the scheme is missing from the PROVURL parameter, then “http” is assumed.

CONTEXT-ALLOW (0 or 1 entries)

The CONTEXT-ALLOW parameter defines how many additional configuration contexts the privileged context allows to the ME to support. If the parameter is present but no value is given, the default value 0 should be assumed. If the parameter is omitted it has no impact on the number of configuration contexts allowed. It may have the following values:

Value	Meaning
0	No other configuration context than the privileged context is allowed (default)
1...254	Describes how many ADDITIONAL configuration contexts beyond the privileged context are allowed. If the value exceeds the maximum number of supported contexts of the ME, the maximum number of supported contexts is used instead
255	Allows for the use of the maximum number of configuration contexts the ME supports

4.6.9 Parameters for CLIENTIDENTITY characteristics

The CLIENTIDENTITY characteristics may be used to provide ME identity. Note that the parameters listed below are described in the scope of this particular characteristic.

Names and values of parameters

CLIENT-ID

The identifier of the mobile device, which for example could be the assigned-client-id as defined in [CLIENTID]. The parameter CLIENT-ID MUST NOT be defined more than once in a configuration context as it is global within the context. For rules on the usage of this parameter see [ProvUAB] section 4.7.

4.6.10 Parameters for VENDORCONFIG characteristics

The VENDORCONFIG characteristics may be used to provide (ME) vendor specific configuration parameters. Note that the parameters listed below are described in the scope of this particular characteristic.

Names and values of parameters

NAME

The name of the product. The NAME MUST be unique within its enclosed structure, i.e. within the configuration context.

The actual configuration data is provided by means of vendor specific parameter names and values.

4.6.11 Parameters for APPLICATION characteristics

The APPLICATION characteristic provides parameters that a WAP client needs to access a particular application service access point. This may be, for example, a particular MMS Proxy-Relay or some e-mail server. The APPLICATION characteristic is linked to proxy and network access point definitions that are appropriate in the case of this particular application service point. Note that the parameters listed below are described in the scope of this particular characteristic.

If this characteristic is supported the WAP client MUST support the parameters APPID, PROVIDER-ID and ADDR, as well as inclusion of APPADDR characteristics.

Names and values of parameters

APPID

- The APPID identifies the type of the application service available at the described application service access point. The value is expected to be globally unique. . The value is assigned and registered with Open Mobile Naming Authority (OMNA). Details on available names and older registrations are available on OMNA [OMNA] site

PROVIDER-ID (0 or 1 entries)

The PROVIDER-ID parameter provides an identifier for the application service access point described by an APPLICATION characteristic. Two APPLICATION characteristics with the same APPID values but different PROVIDER-ID values MUST be considered to refer to two different application service access points. This parameter may also provide a globally unique external identification of the access point. If the parameter is omitted, the APPLICATION characteristic MUST be considered to describe an anonymous application service access point, which is not the same as the ones with an explicit PROVIDER-ID.

NAME (0 or 1 entries)

The NAME indicates a logical, user readable, identity (property) of the APPLICATION.

AACCEPT (0 or 1 entries)

The AACCEPT parameter lists the content types that the server is able to receive from the client. The value is a string containing a comma-separated list of content type specifiers. The values are in a preference order, with the content type most preferred by the server as the first entry. If this value is omitted, the supported values are discovered in some other manner.

A content type specifier is composed of a type indicator and an optional list of content type version numbers. The following kinds of type indicators are available:

- WSP content type codes maintained by WINA [WINA]. These type indicators are encoded as a string with the hexadecimal representation of the registered numeric content type code. A WAP client MUST recognise these values.
- MIME media type values [RFC2045].
- SGML public identifiers used in the DOCTYPE declaration of XML documents.

The list of content type version numbers is composed of values separated by semicolons ";". The values are in a preference order, with the version most preferred by the server as the first entry. The used version numbering scheme depends on the application, but use of '1*DIGIT "." 1*DIGIT' [RFC2234] is recommended.

APROTOCOL (0 or 1 entries)

The APROTOCOL indicates the application protocol versions supported by the server. The value is a string containing a comma-separated list of protocol identifiers. The values are in a preference order, with the protocol most preferred by the server as the first entry. If this value is omitted, the supported values are discovered in some other manner. The formats of the protocol identifiers and the recognised values depend on the used application protocol. This information SHOULD be included in the provisioning parameter registration done with WINA, see section 4.6.

TO-PROXY (0 or more entries)

The TO-PROXY parameter refers to a logical proxy with a matching PROXY-ID. Several TO-PROXY parameters may be listed for a given application. The order of the list indicates the priority of the proxies. However, client preferences MAY also be considered which might affect the priority order (see also [PROVUAB]).

This parameter MUST be supported by the WAP client, if it is able to use proxies.

TO-NAPID (0 or more entries)

The TO-NAPID parameter refers to a network access point with a matching NAPID parameter. It is only possible to refer to network access points defined within the same provisioning document (except if the INTERNET attribute is set in the NAPDEF). Several TO-NAPID parameters may be listed for a given application. The order of the list indicates the priority of the individual network access points. However, client preferences MAY also be considered which might affect the priority order (see also [PROVUAB]). One TO-NAPID has a special predefined meaning. If the TO-NAPID is INTERNET, it implies that the ME can select any network access point with the attribute INTERNET defined.

This parameter MUST be supported by the WAP client, if it is able to communicate without a proxy.

ADDR (0 or more entries)

The ADDR parameter may be used to provide the address of the application server. The value can be an absolute URI [RFC2396], an IPv4 address [RFC791] represented in decimal format with dots as delimiters, or a fully qualified Internet domain name (i.e. *hostname* as defined in section 3.2.2 of [RFC2396]). The presence of this parameter is equivalent to including an APPADDR characteristic containing only the ADDR parameter with the same value.

4.6.12 Parameters for APPADDR characteristics

The APPADDR characteristic provides the address used to contact the application service access point. It is possible to have multiple alternative addresses for the same access point.

If this characteristic is supported, the WAP client MUST support the parameters ADDR and ADDRTYPE, as well as inclusion of PORT characteristics.

Names and values of parameters

ADDR

The ADDR parameter can hold addresses of different kinds, for example, an IP address or an SME number. The type of address in the field can be determined based on the ADDRTYPE parameter. If the parameter ADDRTYPE is not present or if no value is given, then the parameter ADDR can contain the same type of values as the ADDR parameter in the APPLICATION characteristic, see section 4.6.11.

Value of ADDRTYPE	Content of ADDR
IPV6	An IPv6 address [RFC2373] represented as hexadecimal numbers with colons as delimiters or as a combination of hexadecimal and decimal numbers with dots and colons as delimiters
E164	A phone number according to the E164 scheme [GENFORM]
ALPHA	Generic alphanumeric address (as defined by *alphanum* in [RFC2396])

ADDRTYPE (0 or 1 entries)

The ADDRTYPE indicates the format and interpretation of the ADDR parameter.

4.6.13 Parameters for APPAUTH characteristics

The APPAUTH characteristic provides authentication information to be used with the application service access point.

If this characteristic is supported, the WAP client MUST support the parameters AAUTHLEVEL, AAUTHTYPE, AAUTHNAME and AAUTHSECRET.

Names and values of parameters

AAUTHLEVEL (0 or 1 entries)

The AAUTHLEVEL parameter tells how the provided authentication credentials are to be applied. If the parameter is not present or if no value is given, then authentication at the application protocol level is implied.

Value	Meaning
APPSRV	Authentication done by the application service
OBEX	OBEX authentication [OBEX]

AAUTHTYPE (0 or 1 entries)

The AAUTHTYPE parameter indicates the authentication method used by the application. The value is a string containing a comma-separated list of authentication method identifiers. The values are in a preference order, with the method most preferred by the server as the first entry. The same credentials (AAUTHNAME and

AAUTHSECRET) may be used with any of the listed authentication methods. If none of the listed methods are supported, the WAP client MUST NOT send the provided credentials to the server to avoid compromising them. If this parameter is omitted, the used method depends on the challenge sent by the server or is the default authentication mechanism defined by the application protocol.

Applications may choose to use their own authentication method identifiers, but the following ones are predefined:

Value	Meaning
HTTP-BASIC	Basic authentication done according to [RFC2617]
HTTP-DIGEST	Digest authentication done according to [RFC2617]
BASIC	The 'basic' authentication method recognised by the application
DIGEST	The 'digest' authentication method recognised by the application

AAUTHNAME (0 or 1 entries)

The AAUTHNAME parameter provides the id (plaintext) used in authenticating the user. The format and use of this parameter depend on AAUTHLEVEL and AAUTHTYPE.

AAUTHSECRET (0 or 1 entries)

The AAUTHSECRET provides the authentication secret used in authenticating the user. The format and use of this parameter depend on AAUTHLEVEL and AAUTHTYPE.

AAUTHDATA (0 or 1 entries)

The AAUTHDATA provides additional authentication parameters used in authenticating the user. The format and use of this parameter depend on AAUTHLEVEL and AAUTHTYPE.

4.6.14 Parameters for RESOURCE characteristics

The RESOURCE characteristic indicates the available resources and their access parameters within the APPLICATION characteristic. The resources could be, for example, synchronisable databases or mailboxes.

If this characteristic is supported, the WAP client MUST support the parameters URI and STARTPAGE. If any of AAUTHTYPE, AAUTHNAME and AAUTHSECRET is supported within this characteristic, all of them MUST be supported.

Names and values of parameters

URI

The URI parameter specifies the value used to identify the resource in the application protocol. It may be any string, but often is a relative or absolute URI [RFC2396].

NAME (0 or 1 entries)

The NAME indicates a user readable identity of the RESOURCE.

AACCEPT (0 or more entries)

The definition of this parameter is the same as for the APPLICATION characteristic except that it defines the content types that the server is able to accept when the client is accessing this particular RESOURCE.

AAUTHTYPE (0 or 1 entries)

The definition of this parameter is the same as for the AAUTHTYPE defined in the APPAUTH characteristic except that the authentication parameters are used only when the WAP client accesses the RESOURCE described by this characteristic.

AAUTHNAME (0 or 1 entries)

The AAUTHNAME parameter provides the id (plaintext) used in authenticating the user. The format and use of this parameter depend on AAUTHTYPE.

AAUTHSECRET (0 or 1 entries)

The AAUTHSECRET provides the authentication secret used in authenticating the user. The format and use of this parameter depend on AAUTHTYPE.

AAUTHDATA (0 or 1 entries)

The AAUTHDATA provides additional authentication parameters used in authenticating the user. The format and use of this parameter depend on AAUTHTYPE.

STARTPAGE (0 or 1 entries)

The presence of the STARTPAGE parameter indicates the resource to be one that the user agent is expected to access or select when it first starts accessing the application server. In particular, it may indicate the home page of a browser. This parameter does not take a value.

4.6.15 Parameters for ACCESS characteristic

The ACCESS characteristic defines a list of rules for directing applications to a suitable proxy or network access point. Within the ACCESS characteristic are two sets of parameters interpreted by the user agent that are:

- *access-rule parameters*: used for defining access conditions in which access is granted. A group of access-rule parameters are named an *access rule*. One or more access rules may exist in a single ACCESS characteristic
- *access-result parameters*: used for describing the access granted when an access rule is satisfied. A group of access-result parameters is named an *access result*. Only one access result may exist in a single ACCESS characteristic.

Access-rule parameters define particular applications, port numbers, domain names and URLs that are allowed access to particular NAPDEFs or proxies defined in the access result.

Some of the parameters in the ACCESS characteristic are duplicates of parameters found in other characteristics and take on the same format. Several of these duplicated parameters refer the user agent to the connectivity information elsewhere in the provisioning document.

The user agent's treatment of the parameters in the ACCESS characteristic is covered in [PROVUAB]. This will provide information on the correct formatting of access rules.

The WAP client MUST support the parameters RULE, APPID, PORTNBR and DOMAIN.

Names and values of parameters

RULE (1 or more entries)

RULE is used to delimit individual access-rules. This parameter MAY take a value in order to label an access rule. The RULE parameter value MUST be unique within the enclosed provisioning document. A RULE parameter MUST be positioned at the start of an access rule.

APPID (0 or more entries)

In an ACCESS characteristic, this is classed as an "access-rule parameter" and uses the same format as the APPID parameter in the APPLICATION characteristic. The intention of this parameter is to identify an application service that will be used when forming a mapping to an access-result. Multiple APPID parameters may be included in an access-rule.

PORTNBR (0 or more entries)

In an ACCESS characteristic, this is classed as an "access-rule parameter" and uses the same format as the PORTNBR parameter in the PORT characteristic. The intention of this parameter is to identify a port number that will be used when forming a mapping to an access-result. Multiple PORTNBR parameters may be included in an access-rule.

DOMAIN (0 or more entries)

In an ACCESS characteristic, this is classed as an "access-rule parameter" and uses the same format as the DOMAIN parameter in the PXLOGICAL characteristic. The intention of this parameter is to identify a DOMAIN or URI that will be used when forming a mapping to an access-result. Multiple DOMAIN parameters may be included in an access-rule.

TO-NAPID (0 or more entries)

In an ACCESS characteristic, this is classed as an "access-result parameter" and refers to network access points with matching NAPID parameters in the order of decreasing priority. It is only possible to refer to network access points defined within the same provisioning document (except if the INTERNET attribute is set in the NAPDEF). This parameter indicates the network access point that will be used when the application fully satisfies one of the access rules in the same characteristic.

If the TO-NAPID is INTERNET, it implies that the ME can select any network access point with the attribute INTERNET defined.

The TO-NAPID parameter MUST be present when a direct-access is intended. The WAP client MUST support this parameter, if it is able to support direct access.

TO-PROXY (0 or more entries)

In an ACCESS characteristic, this is classed as an "access-result parameter" and refers to proxies with a matching PROXY-ID parameter in the order of decreasing priority. This parameter indicates a proxy that will be used when the application fully satisfies one of the access rules in the same characteristic. The WAP client MUST support this parameter, if it is able to use proxies.

The [PROVUAB] specification provides detailed information on the usage of these parameters.

4.7 Provisioning Document Character Set

The provisioning document uses an XML language. It inherits the XML document character set and the rules for handling from XML [XML]. Provisioning documents MUST be encoded using UTF-8 [RFC2279]. Numeric character entities are supported, as well as the predefined entities `amp`, `lt`, `gt`, `apos`, `quot` that XML processors MUST recognise.

5. Well Formed Provisioning Documents

5.1 The Length of Parameter Fields

The parameter length definitions in the table below express a minimum requirement on the Provisioning Agent and for every supported parameter the minimum length MUST be supported. The Provisioning Server can assume that parameters with a length shorter or equal to the definitions will be accepted (and stored) by the device.

Name	Length (byte)
AACCEPT	16
AAUTHNAME	16
AAUTHSECRET	16
ADDR	64
APPID	16
APROTOCOL	16
AUTHNAME	16
AUTHSECRET	16
BASAUTH-ID	16
BASAUTH-PW	16
CLIENT-ID	32
DNLINKSPEED	6
DNS-ADDR	15 *)
DOMAIN	64
LINGER	4
LINKSPEED	6
NAME	16
NAP-ADDRESS	16 *) **)
NAPID	16
PHYSICAL-PROXY-ID	16
PROVIDER-ID	32
PROVURL	64
PROXY-ID	32 *)
PROXY-PROVIDER-ID	32 *)
PROXY-PW	16
PXADDR	40 *)
PXADDR-FQDN	64
PXAUTH-ID	16
PXAUTH-PW	16
REREG-THRESHOLD	2
RULE	16
STARTPAGE	64
URI	64
VALIDUNTIL	8

*) If IPV6 is supported the minimum length requirement is 45 bytes.

**) The default dialstring is 16 bytes, but in networks where calling cards can be used the user agent has to support 64 bytes. Also GPRS terminals have to support 64 byte dialstrings.

5.2 The use of PORT characteristics

The total set of port bindings available for a given physical proxy is the port bindings defined for the logical proxy, appended with the port bindings given within the PXPHYSICAL characteristic.

5.3 Missing VALIDITY characteristics

If a VALIDITY characteristic is absent inside a NAPDEF characteristic, the NAP definition is always valid.

6. Examples

This section is informative only.

6.1 Example 1

This example shows a provisioning document containing infrastructure information related to a single logical and physical WSP proxy for a service domain with a single access point.

```
<?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="170.187.51.4"/>
   <parm name="NAME" value="BankMainProxy"/>
   <parm name="STARTPAGE" value="http://www.bank.com/startpage.wml"/>
   <characteristic type="PXAUTHINFO">
     <parm name="PXAUTH-TYPE" value="HTTP-BASIC"/>
     <parm name="PXAUTH-ID" value="pxusername"/>
     <parm name="PXAUTH-PW" value="pxuserpassw"/>
   </characteristic>
   <characteristic type="PXPHYSICAL">
     <parm name="PHYSICAL-PROXY-ID" value="PROXY 1"/>
     <parm name="DOMAIN" value="www.bank.com/"/>
     <parm name="PXADDR" value="170.187.51.3"/>
     <parm name="PXADDRTYPE" value="IPV4"/>
     <parm name="TO-NAPID" value="INTERNET"/>
     <parm name="TO-NAPID" value="NAP1"/>
     <characteristic type="PORT">
       <parm name="PORTNBR" value="9203"/>
     </characteristic>
   </characteristic>
 </characteristic>

 <characteristic type="NAPDEF">
   <parm name="NAPID" value="NAP1"/>
   <parm name="BEARER" value="GSM-CSD"/>
   <parm name="NAME" value="MY ISP CSD"/>
   <parm name="NAP-ADDRESS" value="+35808124002"/>
   <parm name="NAP-ADDRTYPE" value="E164"/>
   <parm name="CALLTYPE" value="ANALOG-MODEM"/>
   <characteristic type="NAPAUTHINFO">
     <parm name="AUTHTYPE" value="PAP"/>
     <parm name="AUTHNAME" value="wwwmmmuser"/>
     <parm name="AUTHSECRET" value="wwwmmmsecret"/>
   </characteristic>
   <characteristic type="VALIDITY">
     <parm name="COUNTRY" value="228"/>
     <parm name="NETWORK" value="001"/>
   </characteristic>
 </characteristic>
```

```
</wap-provisioningdoc>
```

6.2 Example 2

Infrastructure information with two bearers and thus two network access points.

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

<wap-provisioningdoc version="1.1">

 <characteristic type="PXLOGICAL">
   <parm name="PROXY-ID" value="170.187.51.4"/>
   <parm name="NAME" value="DefaultProxy"/>
   <parm name="STARTPAGE" value="http://www.operator.com/start.wml"/>
   <characteristic type="PXAUTHINFO">
     <parm name="PXAUTH-TYPE" value="HTTP-BASIC"/>
     <parm name="PXAUTH-ID" value="pxusername"/>
     <parm name="PXAUTH-PW" value="pxuserpassw"/>
   </characteristic>
   <characteristic type="PXPHYSICAL">
     <parm name="PHYSICAL-PROXY-ID" value="PROXY 1"/>
     <parm name="DOMAIN" value=" "/>
     <parm name="PXADDR" value="221.125.51.4"/>
     <parm name="PXADDRTYPE" value="IPV4"/>
     <parm name="PXADDR-FQDN" value="proxy1.operator.com"/>
     <parm name="TO-NAPID" value="NAP1"/>
     <characteristic type="PORT">
       <parm name="PORTNBR" value="9203"/>
     </characteristic>
   </characteristic>
   <characteristic type="PXPHYSICAL">
     <parm name="PHYSICAL-PROXY-ID" value="PROXY 2"/>
     <parm name="DOMAIN" value="/SMSContent/"/>
     <parm name="DOMAIN" value="sms.operator.com/"/>
     <parm name="PXADDR" value="9400410"/>
     <parm name="PXADDRTYPE" value="E164"/>
     <parm name="TO-NAPID" value="NAP2"/>
     <characteristic type="PORT">
       <parm name="PORTNBR" value="9201"/>
     </characteristic>
   </characteristic>
 </characteristic>

 <characteristic type="NAPDEF">
   <parm name="NAPID" value="NAP1"/>
   <parm name="BEARER" value="GSM-CSD"/>
   <parm name="NAME" value="ANY NAME 1"/>
   <parm name="NAP-ADDRESS" value="+4520671023"/>
   <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="roamwapuser"/>
      <parm name="AUTHSECRET" value="roamwappassw"/>
    </characteristic>
    <characteristic type="VALIDITY">
      <parm name="COUNTRY" value="228"/>
    </characteristic>
 </characteristic>

 <characteristic type="NAPDEF">
    <parm name="NAPID" value="NAP2"/>
    <parm name="BEARER" value="GSM-SMS"/>
    <parm name="NAME" value="ANY NAME 2"/>
    <parm name="NAP-ADDRESS" value="+35809503401"/>
    <parm name="NAP-ADDRTYPE" value="E164"/>
 </characteristic>

</wap-provisioningdoc>
```

In the above example, bearer selection policies for GSM-CSD and GSM-SMS are shown.

The document provides information on how to access the default gateway via two NAP's. Note that complete information on NAP's as well as the physical proxies is given since it is not known in advance how much knowledge the ME has about the infrastructure.

6.3 Example 3

Infrastructure information related to several logical WSP proxies for a service domain with multiple access points. Vendor specific configuration data is also supplied. This situation is typically encountered when fetching provisioning documents from a smart card [PROVSC].

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

<wap-provisioningdoc version="1.1">

 <characteristic type="PXLOGICAL">
    <parm name="PROXY-ID" value="www.operator.com"/>
    <parm name="PROXY-PW" value="proxypasswd"/>
    <parm name="PPGAUTH-TYPE" value="HTTP-BASIC"/>
    <parm name="NAME" value="DefaultProxy"/>
    <parm name="MASTER"/>
    <parm name="PUSHENABLED" value="1"/>
    <parm name="STARTPAGE" value="http://www.operator.com/start.wml"/>
    <characteristic type="PXAUTHINFO">
      <parm name="PXAUTH-TYPE" value="HTTP-BASIC"/>
      <parm name="PXAUTH-ID" value="httpusername"/>
      <parm name="PXAUTH-PW" value="httpuserpassw"/>
    </characteristic>
    <characteristic type="PXPHYSICAL">
      <parm name="PHYSICAL-PROXY-ID" value="PROXY 1"/>
      <parm name="DOMAIN" value=" "/>
      <parm name="PXADDR" value="215.221.51.5"/>
      <parm name="PXADDRTYPE" value="IPV4"/>
      <parm name="TO-NAPID" value="NAP1"/>
```

```
    <characteristic type="PORT">
      <parm name="PORTNBR" value="9203"/>
    </characteristic>
  </characteristic>
  <characteristic type="PXPHYSICAL">
    <parm name="PHYSICAL-PROXY-ID" value="PROXY 2"/>
    <parm name="DOMAIN" value=" "/>
    <parm name="DOMAIN" value="/SMS/"/>
    <parm name="PXADDR" value="9201611"/>
    <parm name="PXADDRTYPE" value="E164"/>
    <parm name="TO-NAPID" value="NAP3"/>
    <characteristic type="PORT">
      <parm name="PORTNBR" value="9201"/>
    </characteristic>
  </characteristic>
</characteristic>

<characteristic type="PXLOGICAL">
  <parm name="PROXY-ID" value="163.187.51.4"/>
  <parm name="NAME" value="EcommerceProxy"/>
  <parm name="STARTPAGE" value="http://www.ecom.com/startpage.wml"/>
  <characteristic type="PXAUTHINFO">
    <parm name="PXAUTH-TYPE" value="HTTP-BASIC"/>
    <parm name="PXAUTH-ID" value="httpusername"/>
    <parm name="PXAUTH-PW" value="httpuserpassw"/>
  </characteristic>
  <characteristic type="PXPHYSICAL">
    <parm name="PHYSICAL-PROXY-ID" value="PROXY 1"/>
    <parm name="DOMAIN" value="www.ecom.com/"/>
    <parm name="PXADDR" value="166.224.1.68"/>
    <parm name="PXADDRTYPE" value="IPV4"/>
    <parm name="TO-NAPID" value="NAP1"/>
    <parm name="TO-NAPID" value="NAP2"/>
    <characteristic type="PORT">
      <parm name="PORTNBR" value="9203"/>
    </characteristic>
  </characteristic>
  <characteristic type="PXPHYSICAL">
    <parm name="PHYSICAL-PROXY-ID" value="PROXY 2"/>
    <parm name="DOMAIN" value="www.ecom.com/SMSContent/"/>
    <parm name="DOMAIN" value="www.ecom.com/SMS/"/>
    <parm name="PXADDR" value="9400410"/>
    <parm name="PXADDRTYPE" value="E164"/>
    <parm name="TO-NAPID" value="NAP3"/>
    <parm name="TO-NAPID" value="NAP4"/>
    <characteristic type="PORT">
      <parm name="PORTNBR" value="9203"/>
    </characteristic>
  </characteristic>
</characteristic>

<characteristic type="NAPDEF">
  <parm name="NAPID" value="NAP1"/>
  <parm name="BEARER" value="GSM-CSD"/>
  <parm name="NAME" value="ANY NAME 3"/>
  <parm name="NAP-ADDRESS" value="+35808124303"/>
```

```
    <parm name="NAP-ADDRTYPE" value="E164"/>
    <parm name="CALLTYPE" value="ANALOG-MODEM"/>
    <characteristic type="NAPAUTHINFO">
      <parm name="AUTHTYPE" value="PAP"/>
      <parm name="AUTHNAME" value="wapuser"/>
      <parm name="AUTHSECRET" value="wappassw"/>
    </characteristic>
    <characteristic type="VALIDITY">
      <parm name="COUNTRY" value="228"/>
      <parm name="NETWORK" value="001"/>
    </characteristic>
  </characteristic>

  <characteristic type="NAPDEF">
    <parm name="NAPID" value="NAP2"/>
    <parm name="BEARER" value="GSM-CSD"/>
    <parm name="NAME" value="ANY NAME 4"/>
    <parm name="NAP-ADDRESS" value="+35808124002"/>
    <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="wwwmmmuser"/>
      <parm name="AUTHSECRET" value="wwwmmmsecret"/>
    </characteristic>
    <characteristic type="VALIDITY">
      <parm name="COUNTRY" value="113"/>
      <parm name="NETWORK" value="004"/>
    </characteristic>
  </characteristic>

  <characteristic type="NAPDEF">
    <parm name="NAPID" value="NAP3"/>
    <parm name="BEARER" value="GSM-SMS"/>
    <parm name="NAME" value="ANY NAME 5"/>
    <parm name="NAP-ADDRESS" value="+35809503401"/>
    <parm name="NAP-ADDRTYPE" value="E164"/>
  </characteristic>

  <characteristic type="NAPDEF">
    <parm name="NAPID" value="NAP4"/>
    <parm name="BEARER" value="GSM-SMS"/>
    <parm name="NAME" value="ANY NAME 6"/>
    <parm name="NAP-ADDRESS" value="+36209400400"/>
  </characteristic>

  <characteristic type="NAPDEF">
    <parm name="NAPID" value="INTERNET"/>
    <parm name="BEARER" value="GSM-GPRS"/>
    <parm name="NAME" value="MY ISP GPRS"/>
    <parm name="NAP-ADDRESS" value="MYISP.gprs"/>
    <parm name="NAP-ADDRTYPE" value="APN"/>
    <parm name="DELIVERY-ERR-SDU" value="3"/>
    <parm name="RESIDUAL-BER" value="70"/>
    <parm name="SDU-ERROR-RATIO" value="6"/>
    <parm name="TRAFFIC-CLASS" value="60"/>
```

```
   <parm name="TRAFFIC-HANDL-PRIO" value="1"/>
   <parm name="MAX-BITRATE-DNLINK" value="8"/>
   <characteristic type="NAPAUTHINFO">
     <parm name="AUTHTYPE" value="PAP"/>
     <parm name="AUTHNAME" value="wwwmmmuser"/>
     <parm name="AUTHSECRET" value="wwwmmmsecret"/>
   </characteristic>
 </characteristic>

 <characteristic type="VENDORCONFIG">
   <parm name="NAME" value="PRODUCT"/>
   <parm name="RINGTONES" value="http://www.sonera.fi/music.wml"/>
 </characteristic>

</wap-provisioningdoc>
```

6.4 Example 4

Bootstrap information.

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

<wap-provisioningdoc version="1.1">

 <characteristic type="BOOTSTRAP">
   <parm name="CONTEXT-ALLOW" value="0"/>
   <parm name="PROVURL" value="http://www.operator.com/TPS/"/>
 </characteristic>


 <characteristic type="PXLOGICAL">
   <parm name="PROXY-ID" value="170.187.51.4"/>
   <parm name="PROXY-PW" value="proxypasswd"/>
   <parm name="PPGAUTH-TYPE" value="HTTP-DIGEST"/>
   <parm name="NAME" value="TrustedProvProxy"/>
   <parm name="TRUST"/>
   <parm name="PUSHENABLED" value="1"/>
   <parm name="STARTPAGE" value="http://www.operator.com/home.wml"/>
   <characteristic type="PXAUTHINFO">
     <parm name="PXAUTH-TYPE" value="HTTP-BASIC"/>
     <parm name="PXAUTH-ID" value="subscribername"/>
     <parm name="PXAUTH-PW" value="subscriberpassw"/>
   </characteristic>
   <characteristic type="PXPHYSICAL">
     <parm name="PHYSICAL-PROXY-ID" value="PROXY 1"/>
     <parm name="DOMAIN" value=".operator.com/"/>
     <parm name="PXADDR" value="221.125.33.5"/>
     <parm name="PXADDRTYPE" value="IPV4"/>
     <parm name="TO-NAPID" value="NAP1"/>
   </characteristic>
   <characteristic type="PXPHYSICAL">
     <parm name="PHYSICAL-PROXY-ID" value="PROXY 2"/>
     <parm name="DOMAIN" value="www.operator.com/"/>
```

```
      <parm name="PXADDR" value="9201612"/>
      <parm name="PXADDRTYPE" value="E164"/>
      <parm name="TO-NAPID" value="NAP2"/>
    </characteristic>
 </characteristic>

 <characteristic type="NAPDEF">
    <parm name="NAPID" value="NAP1"/>
    <parm name="BEARER" value="GSM-CSD"/>
    <parm name="NAME" value="ANY NAME 7"/>
    <parm name="NAP-ADDRESS" value="+35808124303"/>
    <parm name="NAP-ADDRTYPE" value="E164"/>
    <parm name="CALLTYPE" value="ANALOG-MODEM"/>
    <characteristic type="NAPAUTHINFO">
      <parm name="AUTHTYPE" value="PAP"/>
      <parm name="AUTHNAME" value="wapuser"/>
      <parm name="AUTHSECRET" value="wappassw"/>
    </characteristic>
    <characteristic type="VALIDITY">
      <parm name="COUNTRY" value="228"/>
      <parm name="NETWORK" value="001"/>
    </characteristic>
 </characteristic>


 <characteristic type="NAPDEF">
    <parm name="NAPID" value="NAP2"/>
    <parm name="BEARER" value="GSM-SMS"/>
    <parm name="NAME" value="ANY NAME 8"/>
    <parm name="NAP-ADDRESS" value="+35809503401"/>
 </characteristic>

</wap-provisioningdoc>
```

6.5 Example 5

This example shows a provisioning document containing infrastructure information for a client that accesses the internet directly without a proxy.

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

<wap-provisioningdoc version="1.1">

 <characteristic type="NAPDEF">
    <parm name="NAPID" value="INTERNET"/>
    <parm name="BEARER" value="GSM-GPRS"/>
    <parm name="NAME" value="MY ISP GPRS"/>
    <parm name="NAP-ADDRESS" value="MYISP.gprs"/>
    <parm name="NAP-ADDRTYPE" value="APN"/>
 </characteristic>

 <characteristic type="BOOTSTRAP">
    <parm name="CONTEXT-ALLOW" value="0"/>
```

```
   <parm name="PROVURL" value="http://www.operator.com/TPS/"/>
 </characteristic>

</wap-provisioningdoc>
```

6.6 Example 6

This example shows a provisioning document containing network access point information for a client that accesses the internet using CDMA2000-1X-SIMPLE-IP bearer and uses CHAP authentication with PAP fallback.

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

<wap-provisioningdoc version="1.1">

 <characteristic type="NAPDEF">
   <parm name="NAPID" value="INTERNET"/>
   <parm name="BEARER" value="CDMA2000-1X-SIMPLE-IP"/>
   <parm name="NAME" value="MY ISP CDMA2000-1X Simple IP"/>
   <parm name="NAP-ADDRESS" value="166.224.1.1"/>
   <parm name="NAP-ADDRTYPE" value="IPV4"/>
   <characteristic type="NAPAUTHINFO">
     <parm name="AUTHTYPE" value="CHAP"/>
     <parm name="AUTHNAME" value="john@carrier.com"/>
     <parm name="AUTHSECRET" value="xyzabc"/>
   </characteristic>
   <characteristic type="NAPAUTHINFO">
     <parm name="AUTHTYPE" value="PAP"/>
     <parm name="AUTHNAME" value="john@carrier.com"/>
     <parm name="AUTHSECRET" value="xyzabc"/>
   </characteristic>
 </characteristic>

 <characteristic type="BOOTSTRAP">
   <parm name="CONTEXT-ALLOW" value="0"/>
   <parm name="PROVURL" value="http://www.operator.com/TPS/"/>
 </characteristic>

</wap-provisioningdoc>
```

6.7 Example 7

This example shows a provisioning document containing network access point information for a client that accesses the internet using CDMA2000-1X-MOBILE-IP. Two NAPDEF definitions are provided – the first one is for primary HA and the second for secondary HA. Primary/secondary order is determined by the order in which the NAPDEF definition occurs in the document as described in the [ProvUAB] specification. Primary HA uses different NAPAUTHINFO definitions for AAA and HA, and the secondary HA uses the same NAPAUTHINFO definition for both AAA and HA.

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

```
<wap-provisioningdoc version="1.1">

 <characteristic type="NAPDEF">
   <parm name="NAPID" value="INTERNET-PRIMARY"/>
   <parm name="BEARER" value="CDMA2000-1X-MOBILE-IP"/>
   <parm name="NAME" value="MY ISP CDMA2000-1X Mobile IP (Primary)"/>
   <parm name="NAP-ADDRESS" value="166.224.1.1"/>
   <parm name="NAP-ADDRTYPE" value="IPV4"/>
   <parm name="MAX-NUM-RETRY" value="2"/>
   <parm name="FIRST-RETRY-TIMEOUT" value="6"/>
   <parm name="REREG-THRESHOLD" value="30"/>
   <parm name="T-BIT"/>
   <characteristic type="NAPAUTHINFO">
     <parm name="AUTHTYPE" value="MD5"/>
     <parm name="AUTHNAME" value="john@carrier.com"/>
     <parm name="AUTHSECRET" value="ha-xyzabc"/>
     <parm name="AUTH-ENTITY" value="HA"/>
   </characteristic>
   <characteristic type="NAPAUTHINFO">
     <parm name="AUTHTYPE" value="MD5"/>
     <parm name="AUTHNAME" value="john@carrier.com"/>
     <parm name="AUTHSECRET" value="aaa-xyzabc"/>
     <parm name="AUTH-ENTITY" value="AAA"/>
   </characteristic>
 </characteristic>

<characteristic type="NAPDEF">
   <parm name="NAPID" value="INTERNET-BACKUP"/>
   <parm name="BEARER" value="CDMA2000-1X-MOBILE-IP"/>
   <parm name="NAME" value="MY ISP CDMA2000-1X Mobile IP (Secondary)"/>
   <parm name="NAP-ADDRESS" value="166.224.2.1"/>
   <parm name="NAP-ADDRTYPE" value="IPV4"/>
   <parm name="MAX-NUM-RETRY" value="2"/>
   <parm name="FIRST-RETRY-TIMEOUT" value="6"/>
   <parm name="REREG-THRESHOLD" value="30"/>
   <parm name="T-BIT"/>

   <characteristic type="NAPAUTHINFO">
     <parm name="AUTHTYPE" value="MD5"/>
     <parm name="AUTHNAME" value="john@carrier.com"/>
     <parm name="AUTHSECRET" value="xyzabc"/>
     <parm name="AUTH-ENTITY" value="HA"/>
     <parm name="AUTH-ENTITY" value="AAA"/>
   </characteristic>
</characteristic>

 <characteristic type="BOOTSTRAP">
   <parm name="CONTEXT-ALLOW" value="0"/>
   <parm name="PROVURL" value="http://www.operator.com/TPS/"/>
 </characteristic>

</wap-provisioningdoc>
```

6.8 Example 8

This example demonstrates the use of several ACCESS characteristics for comprehensively defining the connectivity for various application conditions. Two GPRS network access points are provided, one accessing an operator's network and the other accessing a corporate network.

The first ACCESS characteristic instructs all applications that uses port 80 (HTTP) for the domain www.corporate.com to access the corporate APN and DNS server, and directs the MMS application to a corporate MMS Proxy-Relay via the corporate APN and DNS server.

The second ACCESS characteristic is a wildcard condition and instructs all applications that use any port to access an operator's APN and proxy. This wildcard excludes port 80 applications and the MMS application, which are given higher priority by the user agent.

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

<wap-provisioningdoc version="1.1">

 <characteristic type="PXLOGICAL">
   <parm name="PROXY-ID" value="www.operator.com"/>
   <parm name="PROXY-PW" value="proxypasswd"/>
   <parm name="PPGAUTH-TYPE" value="HTTP-BASIC"/>
   <parm name="NAME" value="DefaultProxy"/>
   <parm name="MASTER"/>
   <parm name="PUSHENABLED" value="1"/>
   <parm name="STARTPAGE" value="http://www.operator.com/start.wml"/>
   <characteristic type="PXAUTHINFO">
     <parm name="PXAUTH-TYPE" value="HTTP-BASIC"/>
     <parm name="PXAUTH-ID" value="httpusername"/>
     <parm name="PXAUTH-PW" value="httpuserpassw"/>
   </characteristic>
   <characteristic type="PXPHYSICAL">
     <parm name="PHYSICAL-PROXY-ID" value="PROXY 1"/>
     <parm name="DOMAIN" value=" "/>
     <parm name="PXADDR" value="215.221.51.5"/>
     <parm name="PXADDRTYPE" value="IPV4"/>
     <parm name="TO-NAPID" value="NAP1"/>
     <characteristic type="PORT">
       <parm name="PORTNBR" value="9203"/>
     </characteristic>
   </characteristic>
 </characteristic>

 <characteristic type="NAPDEF">
   <parm name="NAPID" value="NAP1"/>
   <parm name="BEARER" value="GSM-GPRS"/>
   <parm name="NAME" value="Access Point 1"/>
   <parm name="NAP-ADDRESS" value="AP1.gprs"/>
   <parm name="NAP-ADDRTYPE" value="APN"/>
   <parm name="DELIVERY-ERR-SDU" value="3"/>
   <parm name="RESIDUAL-BER" value="70"/>
```

```
    <parm name="SDU-ERROR-RATIO" value="6"/>
    <parm name="TRAFFIC-CLASS" value="60"/>
    <parm name="TRAFFIC-HANDL-PRIO" value="1"/>
    <parm name="MAX-BITRATE-DNLINK" value="8"/>
    <characteristic type="NAPAUTHINFO">
      <parm name="AUTHTYPE" value="PAP"/>
      <parm name="AUTHNAME" value="wwwmmmuser"/>
      <parm name="AUTHSECRET" value="wwwmmmsecret"/>
    </characteristic>
  </characteristic>

  <characteristic type="NAPDEF">
    <parm name="NAPID" value="NAP2"/>
    <parm name="BEARER" value="GSM-GPRS"/>
    <parm name="NAME" value="Access Point 2"/>
    <parm name="NAP-ADDRESS" value="AP2.gprs"/>
    <parm name="NAP-ADDRTYPE" value="APN"/>
    <parm name="DNS-ADDR" value="132.12.78.223"/>
    <parm name="DELIVERY-ERR-SDU" value="3"/>
    <parm name="RESIDUAL-BER" value="70"/>
    <parm name="SDU-ERROR-RATIO" value="6"/>
    <parm name="TRAFFIC-CLASS" value="60"/>
    <parm name="TRAFFIC-HANDL-PRIO" value="1"/>
    <parm name="MAX-BITRATE-DNLINK" value="8"/>
    <characteristic type="NAPAUTHINFO">
      <parm name="AUTHTYPE" value="PAP"/>
      <parm name="AUTHNAME" value="anotheruser"/>
      <parm name="AUTHSECRET" value="anothersecret"/>
    </characteristic>
  </characteristic>

  <characteristic type="APPLICATION">
     <parm name="APPID" value="w4"/>
     <parm name="NAME" value="Corporate MMS"/>
     <parm name="ADDR" value="http://mms.corporate.com/mmsc"/>
  </characteristic>

  <characteristic type="ACCESS">
    <parm name="RULE" value="ACCESS1"/>
    <parm name="PORTNBR" value="80"/>
    <parm name="DOMAIN" value="www.corporate.com"/>
    <parm name=”RULE”>
    <parm name="APPID" value="w4"/>
    <parm name="TO-NAPID" value="NAP2"/>
  </characteristic>

  <characteristic type="ACCESS">
    <parm name="RULE" value="ACCESS2"/>
    <parm name="TO-PROXY" value="www.operator.com"/>
  </characteristic>

</wap-provisioningdoc>
```

7. WBXML Encoding

For an example of a WBXML encoded provisioning document see **Error! Reference source not found.**.

7.1 Element tokens

The following token codes represent tags in code page zero (0). All numbers are in hexadecimal.

Tag Name	*Token*
wap-provisioningdoc	5
characteristic	6
parm	7

The following token codes represent tags in code page one (1). All numbers are in hexadecimal.

Tag Name	*Token*
characteristic	6
parm	7

7.2 Attribute Start Tokens

The following token codes represent the start of an attribute in code page zero (0) unless stated otherwise. All numbers are in hexadecimal.

7.2.1 Wap-provisioningdoc Attribute Start Tokens

Attribute Name	*Attribute Value Prefix*	*Token*
version		45
version	1.0	46

7.2.2 Characteristic Attribute Start Tokens

Attribute Name	*Attribute Value Prefix*	*Token*
type		50
type	PXLOGICAL	51
type	PXPHYSICAL	52

Attribute Name	*Attribute Value Prefix*	*Token*
type	PORT	53
type	VALIDITY	54
type	NAPDEF	55
type	BOOTSTRAP	56
type	VENDORCONFIG	57
type	CLIENTIDENTITY	58
type	PXAUTHINFO	59
type	NAPAUTHINFO	5A
type	ACCESS	5B

The token codes in the following table represent tags in code page one (1). All numbers are in hexadecimal.

Attribute Name	*Attribute Value Prefix*	*Token*
type		50
type	PORT	53
type	CLIENTIDENTITY	58
type	APPLICATION	55
type	APPADDR	56
type	APPAUTH	57
type	RESOURCE	59

7.2.3 Parm Attribute Start Tokens

Attribute Name	*Attribute Value Prefix*	*Token*
name		5
value		6
name	NAME	7
name	NAP-ADDRESS	8
name	NAP-ADDRTYPE	9
name	CALLTYPE	A

Attribute Name	*Attribute Value Prefix*	*Token*
name	VALIDUNTIL	B
name	AUTHTYPE	C
name	AUTHNAME	D
name	AUTHSECRET	E
name	LINGER	F
name	BEARER	10
name	NAPID	11
name	COUNTRY	12
name	NETWORK	13
name	INTERNET	14
name	PROXY-ID	15
name	PROXY-PROVIDER-ID	16
name	DOMAIN	17
name	PROVURL	18
name	PXAUTH-TYPE	19
name	PXAUTH-ID	1A
name	PXAUTH-PW	1B
name	STARTPAGE	1C
name	BASAUTH-ID	1D
name	BASAUTH-PW	1E
name	PUSHENABLED	1F
name	PXADDR	20
name	PXADDRTYPE	21
name	TO-NAPID	22
name	PORTNBR	23
name	SERVICE	24
name	LINKSPEED	25
name	DNLINKSPEED	26
name	LOCAL-ADDR	27

Attribute Name	*Attribute Value Prefix*	*Token*
name	LOCAL-ADDRTYPE	28
name	CONTEXT-ALLOW	29
name	TRUST	2A
name	MASTER	2B
name	SID	2C
name	SOC	2D
name	WSP-VERSION	2E
name	PHYSICAL-PROXY-ID	2F
name	CLIENT-ID	30
name	DELIVERY-ERR-SDU	31
name	DELIVERY-ORDER	32
name	TRAFFIC-CLASS	33
name	MAX-SDU-SIZE	34
name	MAX-BITRATE-UPLINK	35
name	MAX-BITRATE-DNLINK	36
name	RESIDUAL-BER	37
name	SDU-ERROR-RATIO	38
name	TRAFFIC-HANDL-PRIO	39
name	TRANSFER-DELAY	3A
name	GUARANTEED-BITRATE-UPLINK	3B
name	GUARANTEED-BITRATE-DNLINK	3C
name	PXADDR-FQDN	3D
name	PROXY-PW	3E
name	PPGAUTH-TYPE	3F
name	PULLENABLED	47
name	DNS-ADDR	48
name	MAX-NUM-RETRY	49
name	FIRST-RETRY-TIMEOUT	4A
name	REREG-THRESHOLD	4B

Attribute Name	*Attribute Value Prefix*	*Token*
name	T-BIT	4C
name	AUTH-ENTITY	4E
name	SPI	4F

The token codes in the following table represent tags in code page one (1). All numbers are in hexadecimal.

Attribute Name	*Attribute Value Prefix*	*Token*
name		5
value		6
name	NAME	7
name	INTERNET	14
name	STARTPAGE	1C
name	TO-NAPID	22
name	PORTNBR	23
name	SERVICE	24
name	AACCEPT	2E
name	AAUTHDATA	2F
name	AAUTHLEVEL	30
name	AAUTHNAME	31
name	AAUTHSECRET	32
name	AAUTHTYPE	33
name	ADDR	34
name	ADDRTYPE	35
name	APPID	36
name	APROTOCOL	37
name	PROVIDER-ID	38
name	TO-PROXY	39
name	URI	3A
name	RULE	3B

7.3 Parameter Token Values

Here, values of parameters, and their tokenization, are defined within each parameter description. The token table is logically divided in different subsections, however the token values are for global use within the attribute Value of the PARM element.

The following token codes represent attribute values in code page zero (0). All numbers are in hexadecimal.

7.3.1 ADDRTYPE Value

Attribute Value	*Token*
IPV4	85
IPV6	86
E164	87
ALPHA	88
APN	89
SCODE	8A
TETRA-ITSI	8B
MAN	8C

The token codes in the following table represent tags in code page one (1). All numbers are in hexadecimal.

Attribute Value	*Token*
IPV6	86
E164	87
ALPHA	88
APPSRV	8D
OBEX	8E

7.3.2 CALLTYPE Value

Attribute Value	*Token*
ANALOG-MODEM	90
V.120	91
V.110	92

Attribute Value	*Token*
X.31	93
BIT-TRANSPARENT	94
DIRECT-ASYNCHRONOUS-DATA-SERVICE	95

7.3.3 AUTHTYPE/PXAUTH-TYPE Value

Attribute Value	*Token*
PAP	9A
CHAP	9B
HTTP-BASIC	9C
HTTP-DIGEST	9D
WTLS-SS	9E
MD5	9F

7.3.4 BEARER Value

Attribute Value	*Token*
GSM-USSD	A2
GSM-SMS	A3
ANSI-136-GUTS	A4
IS-95-CDMA-SMS	A5
IS-95-CDMA-CSD	A6
IS-95-CDMA-PACKET	A7
ANSI-136-CSD	A8
ANSI-136-GPRS	A9
GSM-CSD	AA
GSM-GPRS	AB
AMPS-CDPD	AC
PDC-CSD	AD
PDC-PACKET	AE
IDEN-SMS	AF

Attribute Value	*Token*
IDEN-CSD	B0
IDEN-PACKET	B1
FLEX/REFLEX	B2
PHS-SMS	B3
PHS-CSD	B4
TETRA-SDS	B5
TETRA-PACKET	B6
ANSI-136-GHOST	B7
MOBITEX-MPAK	B8
CDMA2000-1X-SIMPLE-IP	B9
CDMA2000-1X-MOBILE-IP	BA

7.3.5 LINKSPEED Value

Attribute Value	*Token*
AUTOBAUDING	C5

7.3.6 SERVICE Value

Attribute Value	*Token*
CL-WSP	CA
CO-WSP	CB
CL-SEC-WSP	CC
CO-SEC-WSP	CD
CL-SEC-WTA	CE
CO-SEC-WTA	CF
OTA-HTTP-TO	D0
OTA-HTTP-TLS-TO	D1
OTA-HTTP-PO	D2
OTA-HTTP-TLS-PO	D3

7.3.7 AAUTHTYPE Value

The token codes in the following table represent attribute values in code page one (1). All numbers are in hexadecimal.

Attribute Value	*Token*
, (comma character)	90
HTTP-	91
BASIC	92
DIGEST	93

7.3.8 AUTH-ENTITY Value

The token codes in the following table represent attribute values in code page one (0). All numbers are in hexadecimal.

Attribute Value	*Token*
AAA	E0
HA	E1

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
WAP-183-ProvCont-20010724-a	2001-07-24	Approved

A.2 Draft/Candidate Version 1.1 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-xxyyz-V1_2	14-Mar-2001		The initial version of this document.
	24-Jul-2001		Included SINs WAP-183_001-ProvCont-20010614-a and WAP-183_002-ProvCont-20010716-a.
	25-Feb-2002	All	New template.
	20-Sep-2002	Several	Updated for 2.0 compliance. Incorporated SINs WAP-183_003-ProvCont-20010912-a WAP-183_004-ProvCont-20011025-a WAP-183_005-ProvCont-20020411-a.
Candidate Versions	12 Nov 2002	n/a	Address remarks from Architectural Consistency Review. Candidate.
OMA-WAP-TS-ProvCont-V1_1	28 Apr 2005	 7.3.7, 7.3.8 4.6.5, 4.6.6	Template update CR 2003-0021 incorporated CR 2003-0048 incorporated
	19 Sep 2006	2.2, 3.3, 4.6.11	Template update Class 2 CR OMA-DM-2006-0069-CR_CP_ProvCont_OMNAforAPPID incorporated
Draft Versions OMA-WAP-TS-ProvCont-V1_1	05 Oct 2007	All	Updated with agreed CR: OMA-DM-CP-2006-0005
Candidate Versions OMA-WAP-TS-ProvCont-V1_1	26 Feb 2008	n/a	Status changed to Candidate by TP TP ref# OMA-TP-2008-0085-INP_ClientProvisioning_V1_1_ERP_for_Notification

Appendix B. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [IOPPROC].

Client Features

B.1.1. Character Set and Encoding

Item	Function	Ref.	Status	Requirement
ProvCont-CSE-C-001	UTF-8 Encoding.	4.7	M	
ProvCont-CSE-C-002	Character entities.	4.7	M	

B.1.2. Content Format and Tokenization

Item	Function	Ref.	Status	Requirement
ProvCont-CO-C-001	Support for the WAP-PROVISIONINGDOC DTD.	4.1	M	
ProvCont-CO-C-002	Support for WAP-PROVISIONINGDOC in textual form (text/vnd.wap.connectivity-xml).	4.2	O	
ProvCont-CO-C-003	Support for WAP-PROVISIONINGDOC in tokenized form (application/vnd.wap.connectivity-wbxml).	**Error! Reference source not found.**	M	WBXML-C-001 AND WBXML-C-011
ProvCont-CO-C-004	Support for media type parameter MAC	4.3	M	
ProvCont-CO-C-005	Support for media type parameter SEC	4.3	M	

B.1.3. Elements and attributes

Item	Function	Ref.	Status	Requirement
ProvCont-CEA-C-001	Support for the element wap-provisioningdoc	4.4	M	
ProvCont-CEA-C-002	Support for the element characteristic	4.5	M	
ProvCont-CEA-C-003	Support for the element parm	4.6	M	
ProvCont-CEA-C-004	Support for the wap-provisioningdoc attribute “version”	4.4	M	
ProvCont-CEA-C-005	Support for the characteristic attribute “type”	4.5	M	
ProvCont-CEA-C-006	Support for the parm attribute “name”	4.6	M	
ProvCont-CEA-C-007	Support for the parm attribute “value”	4.6	M	

B.1.4. Characteristics

Item	Function	Ref.	Status	Requirement
ProvCont-CC-C-001	Support for the characteristic PXLOGICAL	4.5.1	M	
ProvCont-CC-C-002	Support for the characteristic	4.5.2	M	

Item	Function	Ref.	Status	Requirement
	PXPHYSICAL			
ProvCont-CC-C-003	Support for the characteristic PXAUTHINFO	4.5.3	O	ProvCont-CPA-C-001 AND ProvCont-CPA-C-002 AND ProvUAB-UDP-C-009
ProvCont-CC-C-004	Support for the characteristic NAPDEF	4.5.5	M	
ProvCont-CC-C-005	Support for the characteristic NAPAUTHINFO	4.5.6	O	ProvCont-CNA-C-001 AND ProvCont-CNA-C-002 AND ProvCont-CNA-C-003
ProvCont-CC-C-006	Support for the characteristic PORT	4.5.4, 5.2	M	
ProvCont-CC-C-007	Support for the characteristic VALIDITY	4.5.7	O	ProvCont-CV-C-005 AND (ProvCont-CV-C-001 AND ProvCont-CV-C-002) OR (ProvCont-CV-C-003 AND ProvCont-CV-C-004)
ProvCont-CC-C-008	Support for the characteristic BOOTSTRAP	4.5.8	O	ProvCont-CB-C-002
ProvCont-CC-C-009	Support for the characteristic CLIENTIDENTITY	4.5.9	O	ProvCont-CID-C-001 AND ProvUAB-UDP-C-008
ProvCont-CC-C-010	Support for the characteristic VENDORCONFIG	4.5.10	O	ProvCont-CVC-C-001
ProvCont-CC-C-011	Support for the characteristic APPLICATION	4.5.11	O	ProvCont-CAP-C-001 AND ProvCont-CC-C-012 AND ProvUAB-UDP-C-016
ProvCont-CC-C-012	Support for the characteristic APPADDR	0	O	ProvCont-CAA-C-001
ProvCont-CC-C-013	Support for the characteristic APPAUTH	4.5.12	O	ProvCont-CAU-C-001 AND ProvUAB-UDP-C-009
ProvCont-CC-C-014	Support for the characteristic RESOURCE	4.5.13	O	ProvCont-CRE-C-001
ProvCont-CC-C-015	Support for the characteristic ACCESS	4.5.15	M	ProvUAB-UDP-C-010

B.1.5. Characteristic PXLOGICAL

Item	Function	Ref.	Status	Requirement
ProvCont-CPL-C-001	Support for the parm PROXY-ID	4.6.1	M	ProvCont-MLP-C-005
ProvCont-CPL-C-002	Support for the parm PROXY-PROVIDER-ID	4.6.1	O	ProvCont-MLP-C-021
ProvCont-CPL-C-003	Support for the parm NAME	4.6.1	M	ProvCont-MLP-C-001
ProvCont-CPL-C-004	Support for the parm DOMAIN	4.6.1	M	ProvCont-MLP-C-006
ProvCont-CPL-C-005	Support for the parm TRUST	4.6.1	O	
ProvCont-CPL-C-006	Support for the parm MASTER	4.6.1	O	
ProvCont-CPL-C-007	Support for the parm STARTPAGE	4.6.1	M	ProvCont-MLP-C-010
ProvCont-CPL-C-008	Support for the parm BASAUTH-ID	4.6.1	M	ProvCont-MLP-C-011
ProvCont-CPL-C-009	Support for the parm BASAUTH-PW	4.6.1	M	ProvCont-MLP-C-012

Item	Function	Ref.	Status	Requirement
ProvCont-CPL-C-010	Support for the parm WSP-VERSION	4.6.1	O	
ProvCont-CPL-C-011	Support for the parm PUSHENABLED	4.6.1	O	
ProvCont-CPL-C-012	Support for PORT characteristic within PXLOGICAL	4.5.4	M	ProvUAB-UDP-C-006
ProvCont-CPL-C-013	Support for multiple PORT characteristics within PXLOGICAL	4.5.4	O	
ProvCont-CPL-C-014	Support for the parm PROXY-PW	4.6.1	O	ProvCont-MLP-C-023
ProvCont-CPL-C-015	Support for the parm PPGAUTH-TYPE	4.6.1	O	
ProvCont-CPL-C-016	Support for the parm PULLENABLED	4.6.1	O	

B.1.6. Characteristic PXPHYSICAL

Item	Function	Ref.	Status	Requirement
ProvCont-CPP-C-001	Support for the parm PHYSICAL-PROXY-ID	4.6.2	M	ProvCont-MLP-C-018
ProvCont-CPP-C-002	Support for the parm PXADDR	4.6.2	M	ProvCont-MLP-C-013
ProvCont-CPP-C-003	Support for the parm PXADDRTYPE	4.6.2	M	ProvCont-CPP-C-009 OR ProvCont-CPP-C-010 OR ProvCont-CPP-C-011 OR ProvCont-CPP-C-012
ProvCont-CPP-C-004	Support for the parm TO-NAPID	4.6.2	M	
ProvCont-CPP-C-005	Support for the parm DOMAIN	4.6.2	O	ProvCont-MLP-C-006
ProvCont-CPP-C-006	Support for the parm WSP-VERSION	4.6.2	O	
ProvCont-CPP-C-007	Support for the parm PUSHENABLED	4.6.2	O	
ProvCont-CPP-C-008	Support for the TO-NAPID value “INTERNET”	4.6.2	O	
ProvCont-CPP-C-009	Support for PXADDRTYPE value “IPV4”	4.6.2	O	
ProvCont-CPP-C-010	Support for PXADDRTYPE value “IPV6”	4.6.2	O	
ProvCont-CPP-C-011	Support for PXADDRTYPE value “E164”	4.6.2	O	
ProvCont-CPP-C-012	Support for PXADDRTYPE value “ALPHA”	4.6.2	O	
ProvCont-CPP-C-013	Support for PORT characteristic within PXPHYSICAL	4.5.4	M	ProvUAB-UDP-C-006
ProvCont-CPP-C-014	Support for multiple PORT characteristics within PXPHYSICAL	4.5.4	O	
ProvCont-CPP-C-015	Support for multiple TO-NAPID within one PXPHYSICAL	4.6.2	O	
ProvCont-CPP-C-016	Support for the parm PXADDR-FQDN	4.6.2	O	ProvCont-MLP-C-022 AND ProvUAB-UDP-C-005
ProvCont-CPP-C-017	Support for the parm PULLENABLED	4.6.2	O	

B.1.7. Characteristic PXAUTHINFO

Item	Function	Ref.	Status	Requirement
ProvCont-CPA-C-001	Support for the parm PXAUTH-TYPE	4.6.3	O	ProvCont-CPA-C-004 OR

Item	Function	Ref.	Status	Requirement
				ProvCont-CPA-C-005 OR ProvCont-CPA-C-006
ProvCont-CPA-C-002	Support for the parm PXAUTH-ID	4.6.3	O	ProvUAB-UDP-C-007 AND ProvCont-MLP-C-008
ProvCont-CPA-C-003	Support for the parm PXAUTH-PW	4.6.3	O	ProvCont-MLP-C-009
ProvCont-CPA-C-004	Support for PXAUTH-TYPE value "HTTP-BASIC"	4.6.3	O	ProvCont-CPA-C-003
ProvCont-CPA-C-005	Support for PXAUTH-TYPE value "HTTP-DIGEST"	4.6.3	O	ProvCont-CPA-C-003
ProvCont-CPA-C-006	Support for PXAUTH-TYPE value "WTLS-SS"	4.6.3	O	

B.1.8. Characteristic PORT

Item	Function	Ref.	Status	Requirement
ProvCont-CP-C-001	Support for the parm PORTNBR	4.6.4	M	
ProvCont-CP-C-002	Support for the parm SERVICE	4.6.4	M	ProvCont-CP-C-003 OR ProvCont-CP-C-004 OR ProvCont-CP-C-005 OR ProvCont-CP-C-006 OR ProvCont-CP-C-007 OR ProvCont-CP-C-008 OR ProvCont-CP-C-009 OR ProvCont-CP-C-010 OR ProvCont-CP-C-011 OR ProvCont-CP-C-012
ProvCont-CP-C-003	Support for SERVICE value "CL-WSP"	4.6.4	O	
ProvCont-CP-C-004	Support for SERVICE value "CO-WSP"	4.6.4	O	
ProvCont-CP-C-005	Support for SERVICE value "CL-SEC-WSP"	4.6.4	O	
ProvCont-CP-C-006	Support for SERVICE value "CO-SEC-WSP"	4.6.4	O	
ProvCont-CP-C-007	Support for SERVICE value "CO-SEC-WTA"	4.6.4	O	
ProvCont-CP-C-008	Support for SERVICE value "CL-SEC-WTA"	4.6.4	O	
ProvCont-CP-C-009	Support for SERVICE value "OTA-HTTP-TO"	4.6.4	O	ProvCont-CPL-C-014 AND ProvCont-CPL-C-015
ProvCont-CP-C-010	Support for SERVICE value "OTA-HTTP-TLS-TO"	4.6.4	O	ProvCont-CPL-C-014 AND ProvCont-CPL-C-015
ProvCont-CP-C-011	Support for SERVICE value "OTA-HTTP-PO"	4.6.4	O	ProvCont-CPL-C-014 AND ProvCont-CPL-C-015
ProvCont-CP-C-012	Support for SERVICE value "OTA-HTTP-TLS-PO"	4.6.4	O	ProvCont-CPL-C-014 AND ProvCont-CPL-C-015

B.1.9. Characteristic NAPDEF

Item	Function	Ref.	Status	Requirement
ProvCont-CND-C-001	Support for the parm NAPID	4.6.5	M	ProvCont-MLP-C-019
ProvCont-CND-C-002	Support for the parm BEARER	4.6.5	M	ProvCont-CBS-C-001 OR ProvCont-CBS-C-002 OR ProvCont-CBS-C-003 OR ProvCont-CBS-C-004 OR ProvCont-CBS-C-005 OR ProvCont-CBS-C-006 OR ProvCont-CBS-C-007 OR ProvCont-CBS-C-008 OR ProvCont-CBS-C-009 OR ProvCont-CBS-C-010 OR ProvCont-CBS-C-011 OR ProvCont-CBS-C-012 OR ProvCont-CBS-C-013 OR ProvCont-CBS-C-014 OR ProvCont-CBS-C-015 OR ProvCont-CBS-C-016 OR ProvCont-CBS-C-017 OR ProvCont-CBS-C-018 OR ProvCont-CBS-C-019 OR ProvCont-CBS-C-020 OR ProvCont-CBS-C-021 OR ProvCont-CBS-C-022 OR ProvCont-CBS-C-023 OR ProvCont-CBS-C-024 OR ProvCont-CBS-C-025
ProvCont-CND-C-003	Support for the parm NAME	4.6.5	M	ProvCont-MLP-C-001
ProvCont-CND-C-004	Support for the parm INTERNET	4.6.5	O	
ProvCont-CND-C-005	Support for the parm NAP-ADDRESS	4.6.5	M	ProvCont-MLP-C-002
ProvCont-CND-C-006	Support for the parm NAP-ADDRTYPE	4.6.5	M	ProvCont-CND-C-026 OR ProvCont-CND-C-027 OR ProvCont-CND-C-028 OR ProvCont-CND-C-029 OR ProvCont-CND-C-030 OR ProvCont-CND-C-031 OR ProvCont-CND-C-032 OR ProvCont-CND-C-033
ProvCont-CND-C-007	Support for the parm CALLTYPE	4.6.5	O	ProvCont-CND-C-034 OR ProvCont-CND-C-035 OR ProvCont-CND-C-036 OR ProvCont-CND-C-037 OR ProvCont-CND-C-038 OR ProvCont-CND-C-039
ProvCont-CND-C-008	Support for the parm LOCAL-ADDR	4.6.5	O	ProvCont-CND-C-009
ProvCont-CND-C-009	Support for the parm LOCAL-ADDRTYPE	4.6.5	O	ProvCont-CND-C-040 OR ProvCont-CND-C-041
ProvCont-CND-C-010	Support for the parm LINKSPEED	4.6.5	O	ProvCont-MLP-C-014
ProvCont-CND-C-011	Support for the parm DNLINKSPEED	4.6.5	O	ProvCont-MLP-C-015
ProvCont-CND-C-012	Support for the parm LINGER	4.6.5	O	ProvCont-MLP-C-016
ProvCont-CND-C-013	Support for the parm DELIVERY-ERR-SDU	4.6.5	O	

Item	Function	Ref.	Status	Requirement
ProvCont-CND-C-014	Support for the parm DELIVERY-ORDER	4.6.5	O	
ProvCont-CND-C-015	Support for the parm TRAFFIC-CLASS	4.6.5	O	
ProvCont-CND-C-016	Support for the parm MAX-SDU-SIZE	4.6.5	O	
ProvCont-CND-C-017	Support for the parm MAX-BITRATE-UPLINK	4.6.5	O	
ProvCont-CND-C-018	Support for the parm MAX-BITRATE-DNLINK	4.6.5	O	
ProvCont-CND-C-019	Support for the parm RESIDUAL-BER	4.6.5	O	
ProvCont-CND-C-020	Support for the parm SDU-ERROR-RATIO	4.6.5	O	
ProvCont-CND-C-021	Support for the parm TRAFFIC-HANDL-PRIO	4.6.5	O	
ProvCont-CND-C-022	Support for the parm TRANSFER-DELAY	4.6.5	O	
ProvCont-CND-C-023	Support for the parm GUARANTEED-BITRATE-UPLINK	4.6.5	O	
ProvCont-CND-C-024	Support for the parm GUARANTEED-BITRATE-DNLINK	4.6.5	O	
ProvCont-CND-C-025	Support for multiple BEARER within one NAPDEF	4.6.5	O	
ProvCont-CND-C-026	Support for NAP-ADDRTYPE value “IPV4”	4.6.5	O	
ProvCont-CND-C-027	Support for NAP-ADDRTYPE value “IPV6”	4.6.5	O	
ProvCont-CND-C-028	Support for NAP-ADDRTYPE value “E164”	4.6.5	O	
ProvCont-CND-C-029	Support for NAP-ADDRTYPE value “ALPHA”	4.6.5	O	
ProvCont-CND-C-030	Support for NAP-ADDRTYPE value “APN”	4.6.5	O	
ProvCont-CND-C-031	Support for NAP-ADDRTYPE value “SCODE”	4.6.5	O	
ProvCont-CND-C-032	Support for NAP-ADDRTYPE value “TETRA-ITSI”	4.6.5	O	
ProvCont-CND-C-033	Support for NAP-ADDRTYPE value “MAN”	4.6.5	O	
ProvCont-CND-C-034	Support for CALLTYPE value “ANALOG-MODEM”	4.6.5	O	
ProvCont-CND-C-035	Support for CALLTYPE value “V.120”	4.6.5	O	
ProvCont-CND-C-036	Support for CALLTYPE value “V.110”	4.6.5	O	
ProvCont-CND-C-037	Support for CALLTYPE value “X.31”	4.6.5	O	
ProvCont-CND-C-038	Support for CALLTYPE value “BIT-TRANSPARENT”	4.6.5	O	
ProvCont-CND-C-039	Support for CALLTYPE value “DIRECT-ASYNCHRONOUS-DATA-SERVICE”	4.6.5	O	
ProvCont-CND-C-040	Support for LOCAL-ADDRTYPE value	4.6.5	O	

Item	Function	Ref.	Status	Requirement
	"IPV4"			
ProvCont-CND-C-041	Support for LOCAL-ADDRTYPE value "IPV6"	4.6.5	O	
ProvCont-CND-C-042	Support for the parm DNS-ADDR	4.6.5	O	ProvCont-MLP-C-024
ProvCont-CND-C-043	Support for the parm MAX-NUM-RETRY	4.6.5	O	
ProvCont-CND-C-044	Support for the parm FIRST-RETRY-TIMEOUT	4.6.5	O	
ProvCont-CND-C-045	Support for the parm REREG-THRESHOLD	4.6.5	O	
ProvCont-CND-C-046	Support for the parmT-BIT	4.6.5	O	

B.1.10. Bearers supported within NAPDEF characteristic

Item	Function	Ref.	Status	Requirement
ProvCont-CBS-C-001	Support for BEARER value "GSM-USSD"	4.6.5	O	
ProvCont-CBS-C-002	Support for BEARER value "GSM-SMS"	4.6.5	O	
ProvCont-CBS-C-003	Support for BEARER value "ANSI-136-GUTS"	4.6.5	O	
ProvCont-CBS-C-004	Support for BEARER value "IS-95-CDMA-SMS"	4.6.5	O	
ProvCont-CBS-C-005	Support for BEARER value "IS-95-CDMA-CSD"	4.6.5	O	
ProvCont-CBS-C-006	Support for BEARER value "IS-95-CDMA-PACKET"	4.6.5	O	
ProvCont-CBS-C-007	Support for BEARER value "ANSI-136-CSD"	4.6.5	O	
ProvCont-CBS-C-008	Support for BEARER value "ANSI-136-GPRS"	4.6.5	O	
ProvCont-CBS-C-009	Support for BEARER value "GSM-CSD"	4.6.5	O	
ProvCont-CBS-C-010	Support for BEARER value "GSM-GPRS"	4.6.5	O	
ProvCont-CBS-C-011	Support for BEARER value "AMPS-CDPD"	4.6.5	O	
ProvCont-CBS-C-012	Support for BEARER value "PDC-CSD"	4.6.5	O	
ProvCont-CBS-C-013	Support for BEARER value "PDC-PACKET"	4.6.5	O	
ProvCont-CBS-C-014	Support for BEARER value "IDEN-SMS"	4.6.5	O	
ProvCont-CBS-C-015	Support for BEARER value "IDEN-CSD"	4.6.5	O	
ProvCont-CBS-C-016	Support for BEARER value "IDEN-PACKET"	4.6.5	O	
ProvCont-CBS-C-017	Support for BEARER value "FLEX/REFLEX"	4.6.5	O	

Item	Function	Ref.	Status	Requirement
ProvCont-CBS-C-018	Support for BEARER value “PHS-SMS”	4.6.5	O	
ProvCont-CBS-C-019	Support for BEARER value “PHS-CSD”	4.6.5	O	
ProvCont-CBS-C-020	Support for BEARER value “TETRA-SDS”	4.6.5	O	
ProvCont-CBS-C-021	Support for BEARER value “TETRA-PACKET”	4.6.5	O	
ProvCont-CBS-C-022	Support for BEARER value “ANSI-136-GHOST”	4.6.5	O	
ProvCont-CBS-C-023	Support for BEARER value “MOBITEX-MPAK”	4.6.5	O	
ProvCont-CBS-C-024	Support for BEARER value “CDMA2000-1X-SIMPLE-IP”	4.6.5	O	
ProvCont-CBS-C-025	Support for BEARER value “CDMA2000-1X-MOBILE-IP”	4.6.5	O	ProvCont-CNA-C-006 AND ProvCont-CNA-C-007 AND ProvCont-CNA-C-008 AND ProvCont-CNA-C-009 AND ProvCont-CNA-C-0010 AND ProvCont-MLP-C-033

B.1.11. Characteristic NAPAUTHINFO

Item	Function	Ref.	Status	Requirement
ProvCont-CNA-C-001	Support for the parm AUTHTYPE	4.6.6	O	ProvCont-CNA-C-004 OR ProvCont-CNA-C-005 OR ProvCont-CNA-C-006
ProvCont-CNA-C-002	Support for the parm AUTHNAME	4.6.6	O	ProvCont-MLP-C-003
ProvCont-CNA-C-003	Support for the parm AUTHSECRET	4.6.6	O	ProvCont-MLP-C-004
ProvCont-CNA-C-004	Support for AUTHTYPE value “PAP”	4.6.6	O	
ProvCont-CNA-C-005	Support for AUTHTYPE value “CHAP”	4.6.6	O	
ProvCont-CNA-C-006	Support for AUTHTYPE value “MD5”	4.6.6	O	
ProvCont-CNA-C-007	Support for the parm AUTH-ENTITY	4.6.6	O	
ProvCont-CNA-C-008	Support for the parm SPI	4.6.6	O	
ProvCont-CNA-C-009	Support for AUTH-ENTITY value “AAA”	4.6.6	O	
ProvCont-CNA-C-010	Support for AUTH-ENTITY value “HA”	4.6.6	O	

B.1.12. Characteristic VALIDITY

Item	Function	Ref.	Status	Requirement
ProvCont-CV-C-001	Support for the parm COUNTRY	4.6.7	O	
ProvCont-CV-C-002	Support for the parm NETWORK	4.6.7	O	ProvCont-CV-C-001

Item	Function	Ref.	Status	Requirement
ProvCont-CV-C-003	Support for the parm SID	4.6.7	O	ProvCont-CV-C-004
ProvCont-CV-C-004	Support for the parm SOC	4.6.7	O	
ProvCont-CV-C-005	Support for the parm VALIDUNTIL	4.6.7	O	ProvCont-MLP-C-017
ProvCont-CV-C-006	Support for multiple MNC in NETWORK value field	4.6.7	O	
ProvCont-CV-C-007	Support for multiple SID in SID value field	4.6.7	O	

B.1.13. Characteristic BOOTSTRAP

Item	Function	Ref.	Status	Requirement
ProvCont-CB-C-001	Support for the parm PROVURL	4.6.8	O	ProvCont-MLP-C-007
ProvCont-CB-C-002	Support for the parm CONTEXT-ALLOW	4.6.8	O	
ProvCont-CB-C-003	Support for the parm PROXY-ID	4.6.8	O	ProvCont-MLP-C-005
ProvCont-CB-C-004	Support for parm NETWORK	4.6.8	O	ProvCont-CB-C-005
ProvCont-CB-C-005	Support for parm COUNTRY	4.6.8	O	
ProvCont-CB-C-006	Support for the parm NAME	4.6.8	O	ProvCont-MLP-C-001

B.1.14. Characteristic CLIENTIDENTITY

Item	Function	Ref.	Status	Requirement
ProvCont-CID-C-001	Support for parm CLIENT-ID	4.6.9	O	ProvUAB-UDP-C-008 AND ProvCont-MLP-C-020

B.1.15. Characteristic VENDORCONFIG

Item	Function	Ref.	Status	Requirement
ProvCont-CVC-C-001	Support for parm NAME	4.6.10	O	ProvCont-MLP-C-001
ProvCont-CVC-C-002	Support for other parameters than NAME	4.6.10	O	

B.1.16. Characteristic APPLICATION

Item	Function	Ref.	Status	Requirement
ProvCont-CAP-C-001	Support for the parm APPID	4.6.11	O	ProvCont-CAP-C-002 AND (ProvCont-CAP-C-006 OR ProvCont-CAP-C-007) AND ProvCont-CAP-C-008 AND ProvCont-MLP-C-025
ProvCont-CAP-C-002	Support for the parm PROVIDER-ID	4.6.11	O	ProvCont-MLP-C-026
ProvCont-CAP-C-003	Support for the parm NAME	4.6.11	O	
ProvCont-CAP-C-004	Support for the parm AACCEPT	4.6.11	O	ProvCont-MLP-C-031
ProvCont-CAP-C-005	Support for the parm APROTOCOL	4.6.11	O	ProvCont-MLP-C-028
ProvCont-CAP-C-006	Support for the parm TO-PROXY	4.6.11	O	
ProvCont-CAP-C-007	Support for the parm TO-NAPID	4.6.11	O	
ProvCont-CAP-C-008	Support for the parm ADDR	4.6.11	O	ProvCont-MLP-C-027

B.1.17. Characteristic APPADDR

Item	Function	Ref.	Status	Requirement
ProvCont-CAA-C-001	Support for the parm ADDR	4.6.12	O	ProvCont-CAA-C-002 AND ProvCont-MLP-C-027
ProvCont-CAA-C-002	Support for the parm ADDRTYPE	4.6.12	O	

B.1.18. Characteristic APPAUTH

Item	Function	Ref.	Status	Requirement
ProvCont-CAU-C-001	Support for the parm AAUTHLEVEL	4.6.13	O	ProvCont-CAU-C-002
ProvCont-CAU-C-002	Support for the parm AAUTHTYPE	4.6.13	O	ProvCont-CAU-C-003
ProvCont-CAU-C-003	Support for the parm AAUTHNAME	4.6.13	O	ProvCont-CAU-C-004 AND ProvCont-MLP-C-029
ProvCont-CAU-C-004	Support for the parm AAUTHSECRET	4.6.13	O	ProvCont-MLP-C-030
ProvCont-CAU-C-005	Support for the parm AAUTHDATA	4.6.13	O	

B.1.19. Characteristic RESOURCE

Item	Function	Ref.	Status	Requirement
ProvCont-CRE-C-001	Support for the parm URI	4.6.14	O	ProvCont-CRE-C-008 AND ProvCont-MLP-C-032
ProvCont-CRE-C-002	Support for the parm NAME	4.6.14	O	
ProvCont-CRE-C-003	Support for the parm AACCEPT	4.6.14	O	ProvCont-MLP-C-031
ProvCont-CRE-C-004	Support for the parm AAUTHTYPE	4.6.14	O	ProvCont-CRE-C-005 AND ProvCont-CRE-C-006
ProvCont-CRE-C-005	Support for the parm AAUTHNAME	4.6.14	O	ProvCont-CRE-C-004 AND ProvCont-CRE-C-006 AND ProvCont-MLP-C-029
ProvCont-CRE-C-006	Support for the parm AAUTHSECRET	4.6.14	O	ProvCont-CRE-C-004 AND ProvCont-CRE-C-005 AND ProvCont-MLP-C-030
ProvCont-CRE-C-007	Support for the parm AAUTHDATA	4.6.14	O	
ProvCont-CRE-C-008	Support for the parm STARTPAGE	4.6.14	O	

B.1.20 Characteristic ACCESS

Item	Function	Ref.	Status	Requirement
ProvCont-CAC-C-001	Support for the parm RULE	4.6.15	M	ProvCont-MLP-C-034
ProvCont-CAC-C-002	Support for the parm APPID	4.6.15	M	ProvCont-MLP-C-025
ProvCont-CAC-C-003	Support for the parm PORTNBR	4.6.15	M	
ProvCont-CAC-C-004	Support for the parm DOMAIN	4.6.15	M	ProvCont-MLP-C-006
ProvCont-CAC-C-005	Support for parm TO-NAPID and/or parm TO-PROXY	4.6.15	M	ProvCont-CAC-C-006 OR ProvCont-CAC-C-007
ProvCont-CAC-C-006	Support for the parm TO-NAPID	4.6.15	O	
ProvCont-CAC-C-007	Support for the parm TO-PROXY	4.6.15	O	

B.1.21. Minimum Length of parameter fields

Item	Function	Ref.	Status	Requirement
ProvCont-MLP-C-001	Support for minimum length of parm NAME	5.1	O	
ProvCont-MLP-C-002	Support for minimum length of parm NAP-ADDRESS	5.1	M	
ProvCont-MLP-C-003	Support for minimum length of parm AUTHNAME	5.1	O	

Item	Function	Ref.	Status	Requirement
ProvCont-MLP-C-004	Support for minimum length of parm AUTHSECRET	5.1	O	
ProvCont-MLP-C-005	Support for minimum length of parm PROXY-ID	5.1	O	
ProvCont-MLP-C-006	Support for minimum length of parm DOMAIN	5.1	O	
ProvCont-MLP-C-007	Support for minimum length of parm PROVURL	5.1	O	
ProvCont-MLP-C-008	Support for minimum length of parm PXAUTH-ID	5.1	O	
ProvCont-MLP-C-009	Support for minimum length of parm PXAUTH-PW	5.1	O	
ProvCont-MLP-C-010	Support for minimum length of parm STARTPAGE	5.1	M	
ProvCont-MLP-C-011	Support for minimum length of parm BASAUTH-ID	5.1	M	
ProvCont-MLP-C-012	Support for minimum length of parm BASAUTH-PW	5.1	M	
ProvCont-MLP-C-013	Support for minimum length of parm PXADDR	5.1	M	
ProvCont-MLP-C-014	Support for minimum length of parm LINKSPEED	5.1	O	
ProvCont-MLP-C-015	Support for minimum length of parm DNLINKSPEED	5.1	O	
ProvCont-MLP-C-016	Support for minimum length of parm LINGER	5.1	O	
ProvCont-MLP-C-017	Support for minimum length of parm VALIDUNTIL	5.1	O	
ProvCont-MLP-C-018	Support for minimum length of parm PHYSICAL-PROXY-ID	5.1	M	
ProvCont-MLP-C-019	Support for minimum length of parm NAPID	5.1	M	
ProvCont-MLP-C-020	Support for minimum length of parm CLIENT-ID	5.1	O	
ProvCont-MLP-C-021	Support for minimum length of parm PROXY-PROVIDER-ID	5.1	O	
ProvCont-MLP-C-022	Support for minimum length of parm PXADDR-FQDN	5.1	O	
ProvCont-MLP-C-023	Support for minimum length of parm PROXY-PW	5.1	O	
ProvCont-MLP-C-024	Support for minimum length of parm DNS-ADDR	5.1	O	
ProvCont-MLP-C-025	Support for minimum length of parm APPID	5.1	O	
ProvCont-MLP-C-026	Support for minimum length of parm PROVIDER-ID	5.1	O	
ProvCont-MLP-C-027	Support for minimum length of parm ADDR	5.1	O	
ProvCont-MLP-C-028	Support for minimum length of parm APROTOCOL	5.1	O	
ProvCont-MLP-C-029	Support for minimum length of parm AAUTHNAME	5.1	O	
ProvCont-MLP-C-030	Support for minimum length pf parm AAUTHSECRET	5.1	O	
ProvCont-MLP-C-031	Support for minimum length of parm AACCEPT	5.1	O	
ProvCont-MLP-C-032	Support for minimum length of parm URI	5.1	O	
ProvCont-MLP-C-033	Support for minimum length of parm REREG-THRESHOLD	5.1	O	
ProvCont-MLP-C-034	Support for minimum length of parm RULE	5.1	M	

B.2. Server Features

Item	Function	Ref.	Status	Requirement
ProvCont-SG-S-001	Encoding between textual and tokenized version of provisioning content	**Error! Reference source not found.**	M	WBXML-S-001 AND WBXML-S-002 AND WBXML-S-004 AND WBXML-S-005 AND WBXML-S-006 AND WBXML-S-008

Appendix C. Encoding of Provisioning Documents (Informative)

This section gives an example of an encoded provisioning document. It is the document in example 1, section 6.1, that is encoded. Encoding rules are defined in [WBXML] and [WSP], but to simplify reading some of the rules are presented here as well:

- Encoding of a *short integer* require the most significant bit to be set, i.e. 1xxx xxxx
- If an element includes attributes the most significant bit should be set to 1
- If an element includes content the next to most significant bit should be set to 1

The encoded header and document is presented in logical fractions of the token stream together with appropriate descriptions.

If SEC is set to USERPIN and USERPIN equals 1234 the following encoding of the WSP header and the provisioning document in example 1 will apply:

Token stream	Description
0106	WSP header, see [WSP] chapter 8.2: TID (01), PDU Type Push (06)
2f	Headers length, see [WSP] chapter 8.2.4.
1f2d	Content type value length given as "Length-quote Length", see [WSP] chapter 8.4.2.2.
b6	The assigned number for the media type application/vnd.wap.connectivity-wbxml is 36 [WINA]. This is encoded as a *short integer*, see [WSP] chapter 8.4.2.1.
9181	Assigned number for the well-known parameter SEC is 11, see [WSP] table 38. This is encoded as a *short integer*. Chosen security method is USERPIN (1), encoded as a *short integer*.
92	Assigned number for the well-known parameter MAC is 12. This is encoded as a *short integer*.
30424233424235353146 30413933333539454332 39453643454143313434 30453441363137343839	The MAC value, 40 bytes.
00	End-of-string for the encoded MAC value.
03	WBXML version 1.3, see [WBXML] chapter 5.4.
0b	The Public Identifier for "-//WAPFORUM//DTD PROV 1.0//EN" [WINA].
6a	Character set UTF-8, see [WBXML] chapter 5.6. MIBEnum for this is 106 [IANA]. In hexadecimal that is 6a.
05	String table length = 05, see [WBXML] chapter 5.7.

4e41503100	String table: 'N', 'A', 'P', '1', 00
c5	Element wap-provisioningdoc includes attribute and content.
46	Attribute version (46, version 1.0).
01	End of attribute list.
c65101	Characteristic (06) PXLOGICAL (51) includes attribute and content (11xx xxxx) and is ended by an end of attribute list.
871506	Parameter (07) PROXY-ID (15) includes attribute but no content (10xx xxxx). The attribute is the value (06) attribute.
033137302e3138372e35312e340001	The value is an inline string (03), "170.187.51.4". Ends with an end of string (00) and an end of attribute list (01).
8707060342616e6b4d61696e50726f78790001	Parameter (07) NAME (07) with attribute (10xx xxxx) value (06), the inline string (03) "BankMainProxy" (42616e6b4d61696e50726f7879). End of string (00) and end of attribute list (01) ends the token stream.
871c0603687474703a2f2f7777772e62616e6b2e636f6d2f737461727470167652e776d6c0001	Parameter STARTPAGE carrying the inline string value "http://www.bank.com/startpage.wml".
c65901	Characteristic PXAUTHINFO with attribute and content.
8719069c01	Parameter PXAUTH-TYPE carrying the value "HTTP-BASIC".
871a0603707875736572 6e616d650001	Parameter PXAUTH-ID carrying the inline string value "pxusername".
871b0603707875736572 7061737377640001	Parameter PXAUTH-PW carrying the inline string value "pxuserpasswd".
01	End of attribute list, i.e. end of characteristic PXAUTHINFO.
c65201	Characteristic PXPHYSICAL with attribute and content.
872f060350524f585920 310001	Parameter PHYSICAL-PROXY-ID carrying the inline string value "PROXY 1".
871706037777772e6261 6e6b2e636f6d2f0001	Parameter DOMAIN carrying the inline string value "www.bank.com/".
872006033137302e3138 372e35312e330001	Parameter PXADDR carrying the inline string value "170.187.51.3".
8721068501	Parameter PXADDRTYPE carrying the value "IPV4".
87220603494e5445524e45540001	Parameter TO-NAPID carrying the inline string value "INTERNET".
872206830001	Parameter TO-NAPID with string table reference to "NAP1", i.e. offset value 0, see [WBXML] chapter 5.7.
c65301	Characteristic PORT.

87230603393230330001	Parameter PORTNBR carrying the inline string value "9203".
01	End of characteristic PORT.
01	End of characteristic PXPHYSICAL.
01	End of characteristic PXLOGICAL.
c65501	Characteristic NAPDEF.
871106830001	Parameter NAPID with string table reference to "NAP1".
871006aa01	Parameter BEARER carrying the value "GSM-CSD".
870706034d5920495350 204353440001	Parameter NAME carrying the inline string value "MY ISP CSD".
870806032b3335383038 3132343030320001	Parameter NAP-ADDRESS carrying the inline string value "+35808124002".
8709068701	Parameter NAP-ADDRTYPE carrying the value "E164".
870a069001	Parameter CALLTYPE carrying the value "ANALOG-MODEM".
c65a01	Characteristic NAPAUTHINFO.
870c069a01	Parameter AUTHTYPE carrying the value "PAP".
870d06037777776d6d6d 757365720001	Parameter AUTHNAME carrying the inline string value "wwwmmmuser".
870e06037777776d6d6d 7365637265740001	Parameter AUTHSECRET carrying the inline string value "wwwmmmsecret".
01	End of characteristic NAPAUTHINFO.
c65401	Characteristic VALIDITY.
871206033232380001	Parameter COUNTRY carrying the inline string value "228".
871306033030310001	Parameter NETWORK carrying the inline string value "001".
01	End of characteristic VALIDITY.
01	End of characteristic NAPDEF.
01	End of element wap-provisioningdoc, i.e. end of provisioning document.