Provisioning User Agent Behaviour

Version 14-March-2001

Wireless Application Protocol
WAP-185-ProvUAB-20010314-a

A list of errata and updates to this document is available from the WAP Forum™ Web site, http://www.wapforum.org/, in the form of SIN documents, which are subject to revision or removal without notice.

This document is available online in PDF format at http://www.wapforum.org/.

Known problems associated with this document are published at http://www.wapforum.org/.

Comments regarding this document can be submitted to the WAP Forum™ in the manner published at http://www.wapforum.org/.

Document History	
WAP-185-ProvUAB-20010314-a	Current

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 scope for the WAP Forum is to define a set of specifications to be used by service applications. The wireless market is growing very quickly, and reaching new customers and services. To enable operators and manufacturers to meet the challenges in advanced services, differentiation and fast/flexible service creation WAP Forum defines a set of protocols in transport, security, transaction, session and application layers. For additional 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. This specification defines user agent behaviour relating to provisioning. For an overview of the WAP provisioning architecture, see [PROVARCH].

2. Document Status

This document is available online in the following formats:

- PDF format at http://www.wapforum.org/.

2.1 Copyright Notice

2.2 Errata

Known problems associated with this document are published at http://www.wapforum.org/.

2.3 Comments

Comments regarding this document can be submitted to the WAP Forum in the manner published at http://www.wapforum.org/.

3. References

3.1 Normative References

[CREQ] "Specification of WAP conformance requirements", WAP Forum, WAP-221-CREQ, URL: http://www.wapforum.org/

[E2ESEC] "Transport Layer End to End Security Specification", WAP Forum, WAP-187-TransportE2ESEC, URL: http://www.wapforum.org/

[PROVBOOT] "WAP Provisioning Bootstrap Specification", WAP Forum, WAP-184-PROVBOOT, URL: http://www.wapforum.org/

[PROVCONT] "WAP Provisioning Content Type Specification", WAP Forum, WAP-183-PROVCONT, URL: http://www.wapforum.org/

[PROVSC] "WAP Smart Card Provisioning Specification", WAP Forum, WAP-186-PROVSC, URL: http://www.wapforum.org/

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

[RFC2396] "URI Generic Syntax", IETF RFC 2396, URL: http://www.ietf.org /

3.2 Informative References

[PROVARCH] "WAP Provisioning Architecture Overview Specification", WAP Forum, WAP-182-PROVARCH, URL: http://www.wapforum.org/

[WAPARCH] "WAP Architecture Specification", WAP Forum WAP-100-WAPARCH, URL: http://www.wapforum.org/

4. Definitions and Abbreviations

4.1 Terminology

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 [RFC 2119].

4.2 Definitions

This section introduces a terminology that will be used throughout this document. Properties of specific elements are also defined.

Alternative Parameter value
: Some characteristics and parameters can occur multiple times, at the same hierarchical position, in a configuration. The characteristics or parameter is then said to have multiple alternative values.

Bootstrap Document
: A connectivity document with information of relevance to the bootstrap process only.

Bootstrap process (bootstrapping)
: The process by which the unconfigured ME is taken from the initial state to or through the TPS Access State. This process can be system specific.

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

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 addresses and Trusted Provisioning Server URL.

Continuous provisioning
: The process by which the ME is provisioned with further infrastructure information at or after the TPS Access state. The information received during the bootstrap MAY be modified. This process is generic and optional. Continuous implies that the process can be repeated multiple times, but not that it is an ongoing activity.

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.

Network Access Point

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

Pre-configured configuration

A configuration installed at point of manufacturing (or similar point in logistics chain).

Privileged Context

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

Provisioned state

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

Redefined parameter

A redefinition of a characteristic or parameter takes place when the current value is overwritten by a new value, for example when a parameter that is already defined once within a connectivity document, and can occur only once, is given another value. A redefinition would also take place when a parameter that can occur N times is given its N+1 value.

TPS

A TPS, 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.

TPS Access State

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

Trusted Proxy

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

4.3 Abbreviations

For the purposes of this specification the following abbreviations apply.

CB	Cell Broadcast short message service
DNS	Domain Name System
DTD	Document Type Definition
GSM	Global System for Mobile communications
ME	Mobile Equipment

NAP	Network Access Point
PIN	Personal Identification Number
SIM	Subscriber Identity Module
SMS	Short Message Service
TPS	Trusted Provisioning Server
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USERNETWPIN	User Network Personal Identification Number
USERPIN	User Personal Identification Number
USERPINMAC	User Personal Identification Number Message Authentication Code
USSD	Unstructured Supplementary Service Data
USSDC	Unstructured Supplementary Service Data Centre
WAP	Wireless Application Protocol
WCMP	Wireless Control Message Protocol
WIM	WAP Identity Module
XML	Extensible Mark-up Language

5. Interpretation of connectivity document parameters

This section describes the way the user agent must behave on receipt of parameters in a connectivity document (see [PROVCONT] for the contents of the connectivity document).

Not all parameters in the connectivity document are mentioned here; only those parameters whose interpretation needs some clarification are described.

5.1 Intradocument conflict resolution

A document can be syntactically correct, but semantically erroneous. The following generic rules MUST be used by the user agent.

Note: redefinition applies for new values assigned to characteristics or parameters that can only occur once. Alternative value can be given to characteristics or parameters having multiple occurrences. Once the maximum number of instances for a parameter or a characteristic has been reached, then redefinition will apply.

- ignore redundant characteristics
  - if a characteristic is redefined (as opposed to given an alternative value) it MUST be ignored. The original definition must prevail.

- ignore redundant parameters
  - if a parameter is redefined (as opposed to given an alternative value) it MUST be ignored. The original definition must prevail.

- ignore unknown characteristics
  - if a characteristics name is unknown then the characteristic MUST be ignored.

- ignore unknown parameters
  - if a parameter name is unknown then the parameter MUST be ignored.

- ignore unknown values
  - if a parameter value is unknown then the parameter MUST be ignored.

- append proxy definitions
  - if a physical proxy is defined multiple times (same PROXY-ID and PHYSICAL-PROXY-ID) within a document then the latter definition has lower priority. The conflict resolution rules defined for interdocument (section 6) interaction MUST be applied.
  - if a logical proxy is defined multiple times (same PROXY-ID) within a document then the latter definition has lower priority. The conflict resolution rules defined for interdocument (section 6) interaction MUST be applied.

- discard redundant NAP definitions
  if a particular NAP-ID value is used multiple times (to define a NAP) within a document then the latter definition is regarded as illegal.

Illegal definitions are ignored, but the document MUST still be processed.

5.2 Use of connectivity document parameters

Upon interpretation of a connectivity document, the user agent must ignore information that is related to capabilities not supported by the device. This relates to the definition of network access points for bearers that are not supported by the device and the definition of port numbers corresponding to protocol stack configurations that are not supported by the device. The following generic rules MUST be used by the user agent:

- a network access point definition for a bearer that is not supported MUST be ignored

- a physical proxy definition that only contains protocol stack configurations that are not supported MUST be ignored

- a physical proxy definition without a valid network access point definition MUST be ignored

- a logical proxy definition without a valid physical proxy definition MUST be ignored

5.3 Error handling

A connectivity document encoded with an alternate DTD might include elements or attributes that are not recognised by certain user agents. In this situation, a user agent SHOULD use the configuration as if the unrecognised tags and attributes were not present as long as the major version number of the connectivity document is supported. If the major version number isn't supported then the connectivity document MUST be ignored.

A connectivity document encoded with an alternate version might include parameters that are not recognised by certain user agents. In this situation, a user agent SHOULD use the configuration as if the unrecognised parameters and values encoding were not present as long as the major version number is supported. If the major version number isn't supported then the connectivity document MUST be ignored.

If a connectivity document is found to be corrupt, then the User Agent SHOULD ignore the document in question, and not apply any higher level logic to resolve the situation.
If the User Agent finds that a connectivity document must be ignored, then the document is treated as if it would not have existed at all. This means that the User Agent will continue its process to find a valid document. For example, if the document on the GSM-SIM turns out to be invalid, then the User Agent SHOULD try to locate a connectivity document in the next possible location, for example the device memory.

5.4 Parameters for the PXPHYSICAL characteristic

TO-NAPID (1 or more entries)

If, when the user agent is attempting to establish a connection to a proxy, the PXPHYSICAL characteristic contains more than one TO-NAPID parameter, then the user agent SHOULD attempt to establish the bearer to each indicated NAP in turn, starting with the first NAP indicated, until a bearer is successfully established. During this selection process, client side preferences MAY also be considered which might affect the priority order. In some cases for example the end-user might have defined a preferred bearer.

For example, if the NAP associated with the first TO-NAPID parameter does not lead to a successful bearer establishment (e.g. bearer service not supported, remote node busy or not available) then the user agent SHOULD then try and establish the bearer using the NAPDEF associated with the next TO-NAPID in the list. This process SHOULD continue until a bearer is successfully established or all NAP's have been tried.

6. Connectivity Document Interaction

This section describes the behaviour that MUST be executed by the client when handling multiple connectivity documents in a single configuration context. This section applies to any situation where implicit relationship between documents must be resolved (for example SIM/WIM and proxy discovery). Additional rules for document and parameter interaction MAY be defined for example in the scope of continuous provisioning and proxy discovery.

6.1 Implicit Priority

The device (e.g. browser) might read connectivity configurations from several sources, for example from a GSM-SIM card and from the device memory. The SIM has 3 storage locations [PROVSC], and the device a number of storage locations.

As each of these "files" are independent they might contain conflicting information.

The sources of connectivity information have different priority, i.e. based on access order. The priority order is

1. files defined on SIM/WIM or SIM
    a. Bootstrap
    b. Config1
    c. Config2
2. Device

The three files on the smart card all define parts of the same configuration context. The configuration context can even be expanded into memory areas in the device. The areas on the device then have lower priority than the smart card storage.

If the device has pre-configured configurations then these have higher priority than connectivity documents added later to the device.

6.2 Conflict Resolution

The potential conflicts between the individual documents of the configuration context MUST be solved by the following set of simple rules:

1. Always Append; add configurations from the new connectivity document to the already defined set.
2. Never Overwrite already defined parameters; Overlapping parameters are discarded.

Note that some parameters such as CLIENT-ID MUST NOT be defined more than once in a Configuration Context as it is global within the context.

The above rules allow for dynamic extension of the connectivity configuration. For example

- Some parameters such as a logical proxy can be extended in a lower priority "file" ("Bootstrap" extended by "config2"). If a parameter is overlapping with a previous definition the file with the higher priority always prevails.

- Parameter values are inherited; A PXLOGICAL with only the PROXY-ID parameter inherits all parameters from previously defined PXLOGICAL definitions with the same PROXY-ID. By defining the same Proxy in multiple files (using the PROXY-ID as a unique identifier) it is possible to define additional network access points for a proxy, thus "combining" information from multiple files.

7. Proxy Selection

The proxy selection is based upon the network address and the path of the request. This information is normally encoded in the URI that, e.g., the browser is fetching. The request's network address and path are matched against the DOMAIN information encoded in the proxy definition mechanism, resulting in the selection of a single proxy. The selection algorithm is split into three tasks; 1) authority matching, 2) path matching, and 3) selection of the best match.

The scope of the proxy selection is the active configuration context, for example explicitly activated by the user, including navigation documents received via [E2ESEC].

7.1 Authority Matching

A URI is said to match a DOMAIN parameter on the authority (network location) part if the authority part of the URI (A) and the authority part of the DOMAIN parameter (B) satisfies either of the below

1) A and B are both fully qualified host names and match according to a case insensitive match;
2) A is a fully qualified host name and has the form XB (a fully qualified host name), B has the form .b and b conforms to the form of a fully qualified domain name. All matches are case insensitive;
3) B is an empty string;
4) A and B are both complete IP addresses and they are equal;

For example, the authority `x.y.com` matches `.y.com` but does not authority match `y.com`. If the `DOMAIN` authority DNS host name contains a greater number of period-separated domain segments than another `DOMAIN` authority, the match is more precise. For example, `x.y.z.com` matches `.y.z.com` better than `.z.com`. Only those proxy definitions that have DOMAIN parameters matching the URI according to the above SHOULD be considered for the path matching task. If the request URI contains a `port` attribute, it must be ignored in the match. The domain segments MUST be fully defined, i.e. the request `topwww.oper.com` does not match the domain `www.oper.com`.

7.2 Path Matching

A URI is said to match a DOMAIN parameter on the path if

1) The path part of the DOMAIN parameter is empty, or
2) The path part of the DOMAIN parameter matches the beginning of the path part of the URL exactly according to a case sensitive string match.

For example, the path of the request `x/y/z/` matches the DOMAIN path `x/y/` but does not path match `x/w/`. The quality of a match is based on the number of exact case insensitive character matches. For example, the path of the request `x/y/z/` matches `x/y/` better than `x/`, and the path of the request `x/y/z` matches `x/y/z` better than `x/y/`. Only those proxy definitions that have DOMAIN parameters matching the URI according to the above SHOULD be considered for the final task of selecting the best match. The path match MUST be fully defined segments of the path, i.e. the path of the request `x/y/zero` does not match the path of the DOMAIN `x/y/z`.

7.3 Selection of the Best Match

If, during any one of the above described tasks, the list of selected proxies becomes empty, or if the requested URI does not contain a fully qualified domain name as specified in [RFC2396], the match process stops and user agent

MUST apply an implementation dependent algorithm to choose the proxy. In other cases, the proxy having given the best match according to the following rules is selected:

1) If, according to an authority match, match A is better than match B, match B is discarded; otherwise
2) If, according to a path match, match A is better than match B, match B is discarded.

If, after comparing all matches against each other according to the above rules, the list of proxies available to handle the request contains more than one physical proxy definition, the ME SHOULD choose a proxy from the list according to the priority order (elements defined first have higher priority than elements defined later) given in the connectivity document. If the most preferred (physical) proxy can't be accessed then the device MAY try definitions with lower priority. Client side preferences MAY also be considered during this selection process, which might affect the priority order. This relates to preferences for bearers and protocol stack configurations. For example, the end-user might have defined a preferred bearer that results in the selection of a proxy that is accessible by that bearer.

An implementation MAY choose to restructure the above series of tasks to allow for a more efficient proxy selection that does not require the construction of lists of proxies and their associated DOMAIN definitions.

7.4 Destination Match Examples

In the following example, the user agent is programmed with the following bearer selection information:

```
<!-- Criteria #0 -->
<parm name="DOMAIN" value=”sms.op.net”/>
<!-- Criteria #1 -->
<parm name="DOMAIN" value=”.op.net/secure/”/>
<!-- Criteria #2 -->
<parm name="DOMAIN" value=”.op.net/”/>
<!-- Criteria #3 -->
<parm name="DOMAIN" value=”/secure/”/>
<!-- Criteria #4 -->
<parm name="DOMAIN" value=” ”>
```

The following matches will occur:

Request URI	Criteria match
http://sms.op.net/	0, 2, 4
http://xyz.op.net:8000/	2, 4
http://xyz.op.net/	2, 4
http://www.op.net/secure/account/	1, 2, 3, 4
https://xyz.op.net/	2, 4
wsp://sms,16505551212/abc/	4

8. Bootstrapping

There can be several possible bootstrap bearers within a specific network type. For example, in GSM the bootstrap [PROVBOOT] might be done over SMS, USSD, Cell Broadcast or it might even be predefined on the SIM card. As this is possible the relationship between the various types of bootstrap processes is important.

8.1 GSM

The following selection process SHOULD be followed by the ME:

1) Search for bootstrap information in SIM/WIM, if no information is found then continue. Predefined bootstrap on the SIM/WIM card has the highest priority. Priorities between SIM and WIM are specified in the Smart Card Provisioning Specification [PROVSC].
2) Search for persistent bootstrap information in the device, if no information is found then continue.
3) Check whether Provisioning over GSM CB is supported. When registering in the network, read Sysinfo. If no CB at all is being sent out then allow provisioning via other bearers else
   a) Wait for the CB schedule message or read channel 421 directly dependent of what is received first
   b) If the CB schedule message shows that no CB channel for provisioning is available, then ignore CB for bootstrapping and allow bootstrapping via other bearers.
   c) Likewise, if the CB schedule message or the channel 421 has not appeared within two schedule periods, the ME may ignore CB for bootstrapping and allow bootstrapping via other bearers.
   d) If a CB channel for provisioning is available, then read the connectivity document from that channel and the device MAY then stop listening to the CB channel for bootstrap.
   e) If the channel 421 has been found, but no bootstrap message has been received within 5 schedule periods, the ME may ignore the CB for bootstrapping and allow bootstrapping via other bearers.

The point at which ME starts listening to the assigned broadcast channel is implementation dependent. However, as a minimum the ME MUST start listening to the broadcast channel when the WAP environment is initialised.

For GSM USSD it is possible to use the WCMP Echo Request message to find out whether the client supports WAP over GSM USSD or not:

1) The WAP Proxy attached to the USSDC may send a WCMP Echo Request to the ME.
2) If the ME supports USSD as a WAP bearer, then
   a) The ME will reply with a WCMP Echo Reply, after which
   b) The WAP Proxy can allow the TPS to proceed with the bootstrap process via GSM/USSD.
3) Otherwise the WAP Proxy knows that GSM/USSD is not available. It can then let the TPS proceed with the bootstrap process via GSM/SMS.

9. Management of Multiple Contexts

A device may contain one or more configuration contexts of which one MUST be reserved for the privileged configuration context. The privileged configuration context controls whether other configuration contexts are available. Hence, arbitrary parties cannot store/alter information in the privileged context. The user can normally not modify the information in the privileged context, however the user MAY make additions to the privileged context (for example userID and password). Furthermore, the user can modify the information that has been defined by the user.
If the device does support multiple configuration contexts, then it SHOULD implement reliable mechanisms to avoid that the user gets slammed with unwanted contexts.

Only the active configuration context is considered in proxy selection. The active configuration context is selected amongst the configuration contexts available on the device, for example, by the user.

This section does not set requirements for User Agent Behaviour, but recommends a number of methods that can be used to create a good and consistent user experience.

- Only one configuration context can be bootstrapped using methods that rely solely on network PIN (NETWPIN). The NETWPIN is a parameter that can be found in the device. If a context is configured using this method then it is usually the default or privileged configuration context.
- If the device already has a privileged context then a method that rely solely on a network PIN (NETWPIN) cannot establish a new context.
- Each subsequent configuration context SHOULD use some kind of user entered PIN (USERPIN, USERNETWPIN, USERPINMAC) in order to bootstrap the device with additional contexts. This assures that the user is aware of every context that is loaded onto the device.
- A short lived user PIN SHOULD be enforced in the bootstrap process. Each bootstrap event SHOULD cause the device to forget the PIN entered by the user, once it has been used to validate a bootstrap. This ensures that a malicious source cannot use the previously used PIN for another bootstrap even if he would get access to it by stealing or cracking.

The mechanisms above ensures that the user has ultimate control over configurations of his phone, assuming that the user interface of the device provides the necessary management tools.

Appendix A. Static Conformance Requirements

A.1 General User Agent Behaviour features

Item	Function	Reference	Status	Requirement
ProvUAB-U-C-001	Support for the WAP-PROVISIONINGDOC	5	M	
ProvUAB-U- C-002	Support for Proxy Selection	7	O	ProvUAB-UPS-C-001 AND ProvUAB-UPS-C-002 AND ProvUAB-UPS-C-003
ProvUAB-U- C-003	Support for Over the Air Bootstrap	8	O	
ProvUAB-U- C-004	Support for local bootstrap by WIM/SIM	8.1	O	
ProvUAB-U- C-005	Support for Connectivity document conflict resolution.	6.2	M	

A.2 Proxy Selection

Item	Function	Reference	Status	Requirement
ProvUAB-UPS-C-001	Support for authority match	7.1	O	
ProvUAB-UPS-C-002	Support for path match	7.2	O	
ProvUAB-UPS-C-003	Support for best match	7.3	O	

A.3 Conflict resolution

Item	Function	Reference	Status	Requirement
ProvUAB-UCR-C-001	Redundant characteristics ignored	5.1	M	
ProvUAB – UCR-C-002	Redundant parameters ignored	5.1	M	
ProvUAB – UCR-C-003	Unknown characteristics ignored	5.1	M	
ProvUAB – UCR-C-004	Unknown parameters ignored	5.1	M	

Item	Function	Reference	Status	Requirement
ProvUAB – UCR-C-005	Unknown values ignored	5.1	M	
ProvUAB - UCR-C-006	Discard redundant NAP definitions but continue to process document	5.1	M	

A.4 Use of connectivity document parameters

Item	Function	Reference	Status	Requirement
ProvUAB – UDP-C-001	Ignore NAP definition when bearer not supported	5.2	M	
ProvUAB – UDP-C-002	Ignore physical proxy definitions containing only unsupported protocols	5.2	M	
ProvUAB – UDP-C-003	Ignore physical proxy definitions without a valid NAP	5.2	M	
ProvUAB – UDP-C-004	Ignore logical proxy definitions without a valid physical proxy.	5.2	M	

A.5 Error handling

Item	Functionality	Reference	Status	Requirement
ProvUAB – UEH-C-001	Ignore unknown tags and attributes in connectivity document	5.3	O	
ProvUAB – UEH-C-002	Ignore document with unsupported major version number	5.3	M	
ProvUAB – UEH-C-003	Ignore parameters and values that are unrecognised	5.3	O	
ProvUAB – UEH-C-004	Ignore corrupt document	5.3	O	
ProvUAB – UEH-C-005	Look for a valid document when current one is invalid	5.3	O	

A.6 GSM Bootstrap

Item	Function	Reference	Status	Requirement
ProvUAB-UGSM-C-001	Support for bootstrap in GSM	8.1	O	ProvUAB-UGSM-C-002 AND ProvUAB-UGSM-C-003

Item	Function	Reference	Status	Requirement
				AND ProvUAB-UGSM-C-004
ProvUAB-UGSM-C-002	WIM/SIM has higher priority than Cell Broadcast	8.1	O	
ProvUAB-UGSM-C-003	Cell Broadcast has higher priority than SMS/USSD	8.1	O	
ProvUAB-UGSM-C-004	SMS and USSD have equal priority	8.1	O	
ProvUAB-UGSM-C-005	Support for Cell Broadcast in GSM	8.1	O	ProvUAB-UGSM-C-006
ProvUAB-UGSM-C-006	GSM Cell Broadcast channel monitored when WAP initialised	8.1	O	

A.7 Multiple Context Management

Item	Functionality	Reference	Status	Requirement
ProvUAB-UCM-C-001	Support for Privileged Configuration Context	9	M	
ProvUAB - UCM-C-002	User can make additions to Privileged configuration Context	9	O	
ProvUAB-UCM-C-003	NETWPIN bootstrap restricted to single context	9	O	
ProvUAB-UCM-C-004	Support for multiple bootstraps using a User PIN method	9	O	
ProvUAB-UCM-C-005	Support for short lived PIN	9	O	

Appendix B. History and Contact Information

Document history		
Date	**Status**	**Comment**
14-March-2001	Approved	Current
Contact Information http://www.wapforum.org. technical.comments@wapforum.org		