Provisioning User Agent Behaviour

Candidate Version 1.1 – 26 Feb 2008

Open Mobile Alliance

OMA-WAP-ProvUAB-v1_1-20080226-C

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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

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

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

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

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

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

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

Contents

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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. This specification defines user agent behaviour relating to provisioning. For an overview of the WAP provisioning architecture, see [PROVARCH].

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

2. References

2.1 Normative References

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

[E2ESEC] "WAP Transport Layer End-to-end Security". WAP Forum™. WAP-187-TransportE2ESec. URL:http://www.openmobilealliance.org/

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

[PROVBOOT] "Provisioning Bootstrap 1.1". Open Mobile Alliance™. OMA-WAP-ProvBoot-v1_1. URL:http://www.openmobilealliance.org/

[PROVCONT] "Provisioning Content 1.1". Open Mobile Alliance™. OMA-WAP-ProvCont-v1_1. URL:http://www.openmobilealliance.org/

[PROVSC] "Provisioning Smart Card 1.1". WAP Forum™. OMA-WAP-ProvSC-v1_1. URL:http://www.openmobilealliance.org/

[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

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

2.2 Informative References

[PROVARCH] "Provisioning Architecture Overview 1.1". Open Mobile Alliance™. OMA-WAP-ProvArch-v1_1. URL:http://www.openmobilealliance.org/

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

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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

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 or application access document with information of relevance to the bootstrap process only.
Bootstrap Process (Bootstrapping)	The process by which the unconfigured ME is taken from the initial state to or through the TPS Access State. This process can be system specific.
Configuration Context	A Configuration Context is a set of connectivity and application configurations typically associated with a single TPS. However, the Configuration Context can also be independent of any TPS. A TPS can be associated with several Configuration Contexts, but a TPS cannot provision a device outside the scope of the Configuration Contexts associated with that particular TPS. In fact, all transactions related to provisioning are restricted to the Configuration Contexts associated with the TPS.
Connectivity Information	This connectivity information relates to the parameters and means needed to access WAP infrastructure. This includes network bearers, protocols, access point addresses as well as proxy, DNS, and application access addresses and Trusted Provisioning Server URLs.
Continuous Provisioning	The process by which the ME is provisioned with further infrastructure information at or after the TPS Access state. The information received during the bootstrap MAY be modified. This process is generic and optional. Continuous implies that the process can be repeated multiple times, but not that it is an ongoing activity.
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 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.
Pre-configured Configuration	A configuration installed at point of manufacturing (or similar point in logistics chain).
Privileged Configuration 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.
Provisioning document	A particular instance of an XML document encoded according to the provisioning content specification [PROVCONT].
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 provisioning 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.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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.
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.
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.

3.3 Abbreviations

CB	Cell Broadcast short message service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTD	Document Type Definition
GSM	Global System for Mobile communications
HTTP	Hyper Text Transfer Protocol
ME	Mobile Equipment
NAP	Network Access Point
OMA	Open Mobile Alliance
PIN	Personal Identification Number
SIM	Subscriber Identity Module
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
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
WSP	Wireless Session Protocol
XML	eXtensible Mark-up Language

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

4. Interpretation of Provisioning Document Parameters

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

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

4.1 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 **Error! Reference source not found.**) 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 **Error! Reference source not found.**) 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.

4.2 Use of provisioning document parameters

Upon interpretation of a provisioning 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

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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

4.3 Error handling

A provisioning document encoded with an alternative 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 provisioning document is supported. If the major version number isn't supported then the provisioning document MUST be ignored.

A provisioning document encoded with an alternative 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 provisioning document MUST be ignored.

If a provisioning 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 provisioning 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 smart card turns out to be invalid, then the User Agent SHOULD try to locate a provisioning document in the next possible location, for example the device memory.

4.4 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 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.

4.5 Obtaining the proxy address with PXADDR-FQDN

The proxy address MAY be specified as a fully qualified domain name in the parameter PXADDR-FQDN. If the client is able to use a domain name as the proxy address, it MUST attempt to resolve the value of PXADDR-FQDN to obtain the IP address of the proxy. If this fails, the proxy address MAY be obtained from PXADDR or by some other mechanism.

If the client is not able to use a domain name as the proxy address, then the proxy address MUST use the PXADDR, to obtain the IP address of the proxy.

4.6 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. If the resulting set of port bindings is empty, then the ME MUST assume a port and service according to its preferences. Each port can support multiple services. If more than one service is supported then all services must be explicitly defined. An ME implementation MUST reject new port bindings if any inconsistencies occur between the port bindings in the root of the PXLOGICAL or in the root of the PXPHYSICAL characteristics.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

4.7 Use of PXAUTHINFO and CLIENTIDENTITY characteristics

The use of the parameters PXAUTH-ID and CLIENT-ID is defined by the following set of rules, which MUST be used if the parameters are supported:

1. Use parameter PXAUTH-ID if it is present and a value is given
2. Expect user input if parameter PXAUTH-ID is present but no value is given (empty string)
3. If parameter PXAUTH-ID is not present, use parameter CLIENT-ID if it is present and a value is given
4. If parameter PXAUTH-ID is not present and parameter CLIENT-ID is present but no value is given (empty string) then use a possible built-in-device identity. The use of the built-in-device identity MAY be prohibited depending on the client's own privacy policies.
5. If parameters PXAUTH-ID and CLIENT-ID are not present, then user input is expected

If the parameter PXAUTH-PW is missing despite indications from PXAUTH-TYPE that it should be used, then user input is expected.

4.8 Missing authentication credentials

If either AUTHNAME or AUTHSECRET are missing from NAPAUTHINFO despite indications from AUTHTYPE that they should be used, the user MUST be prompted for input for the missing AUTHNAME, AUTHSECRET or both. If AUTHNAME or AUTHSECRET are supposed to be empty strings, it must be explicitly declared by inserting the appropriate AUTHNAME or AUTHSECRET with the value of an empty string into the provisioning document.

If either AAUTHNAME or AAUTHSECRET are missing from APPAUTH despite indications from AAUTHTYPE that they should be used, the user MUST be prompted for input for the missing AAUTHNAME, AAUTHSECRET or both. If AAUTHNAME or AAUTHSECRET are supposed to be empty strings, it must be explicitly declared by inserting the appropriate AAUTHNAME or AAUTHSECRET with the value of an empty string into the provisioning document.

4.9 Provisioning of access models

The ME can access application servers in the Internet either via a WAP Proxy (proxy access model) or directly bypassing the proxy (direct access model). In this context, a WAP Proxy is assumed to provide delegated DNS client functionality.

The ACCESS characteristic specifies proxies or network access points provisioned for a particular application/port/domain mapping. The ACCESS characteristic can contain *access rule parameters* (RULE, APPID, PORTNBR and DOMAIN), and access result parameters (TO-NAPID and TO-PROXY). The RULE parameter delimits and/or labels individual access rules.

The definitions of access-rule parameters and access-result parameters are specified in [PROVCONT].

4.9.1 Access Selection

A network access request is characterised by the application identifier, port number and/or domain relating to that request. Once a match occurs between a network access request and an entry in the list of access rules (derived from the provisioning document), then a connection is made in accordance with the access result associated with the matched access rule. The list of access rules is prioritised according to the access-rule parameter types specified in the access rule as in Section 4.9.1.2.

Multiple parameters of the same type may be included in an access-rule.

For an access rule to be satisfied, the conditions of at least one value of every parameter-type contained within the access-rule must be matched by the network access request. This will grant access in the manner described in the access result associated with the satisfied access rule.

The access selection process for matching the network access request with the DOMAIN parameter in an ACCESS characteristic is found in the Proxy Selection mechanism, see section **Error! Reference source not found.**. Although DOMAIN matching in the Proxy Selection mechanism only applies to URIs, DOMAIN matching in the access selection

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document. [OMA-Template-Spec-20050101-I]

mechanism also applies to domain fields in other application protocols. For example, access selection will allow for Authority Matching of domains in SMTP addresses.

4.9.1.1 Multiple Access Rules in the Same ACCESS Characteristic

A RULE parameter is positioned at the beginning of each access rule and marks the start of a new access rule, thus enabling multiple access rules to pertain to the same access result.

The access result is granted to the application when it satisfies any one of the access-rules in the ACCESS characteristic.

4.9.1.2 Prioritisation

The following list shows the possible combinations of access-rule parameters in an access rule and their interpretations. This lists the prioritisation (from highest to lowest) of access-rule matches that the user agent MUST process when granting access.

1. An access rule with an APPID and PORTNBR and DOMAIN parameter will apply to a particular application using a particular port for a particular domain.
2. An access rule with an APPID and PORTNBR parameter will apply to an application using a particular port for any domain
3. An access rule with a DOMAIN parameter and an APPID will apply to a particular application using any port for a particular domain
4. An access rule with a DOMAIN parameter and a PORTNBR will apply to any application on a particular port for a particular domain
5. An access rule with no DOMAIN parameter and an APPID will apply to a particular application on any port for any domain
6. An access rule with no DOMAIN parameter and a PORTNBR will apply to any application on a particular port for any domain
7. An access rule with only a DOMAIN parameter will apply to all applications and ports for a particular domain.
8. An access rule without APPID, PORTNBR and DOMAIN parameters will apply to all applications and ports for all domains

The ordering of multiple ACCESS characteristics has no implication on the prioritisation of access rules. If multiple access rules have the same priority and conflict, then the latter conflicting access rule in the provisioning document takes priority.

Any TO-NAPID or TO-PROXY for access result in an ACCESS characteristic MUST have a lower priority than those defined for a matched APPID in an APPLICATION characteristic.

DOMAIN parameters in ACCESS characteristics referring to proxies MUST have higher priority than DOMAIN parameters in the PXLOGICAL characteristics of these reference proxies.

4.9.1.3 Multiple Access-result Parameters in an Access Result

Only one access result is contained in each ACCESS characteristic, although several TO-PROXY and/or TO-NAPID parameters may be listed in an access result. The order of parameters in an access result prioritises the means of access, from highest priority to lowest.

4.9.2 Access Selection and Proxy Selection

If the ACCESS characteristic is supported, then the access selection mechanism specified in Section 4.9.1.2 MUST be prioritised over proxy selection. If the access result indicates a proxy access, then the proxy selection mechanism specified in Section **Error! Reference source not found.** applies.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

4.10 Interpretation of APPLICATION characteristics

The APPLICATION characteristic may include TO-PROXY and TO-NAPID parameters. A TO-PROXY parameter tells that the ME is to attempt access through the indicated proxy, while a TO-NAPID indicates that the ME is to attempt direct access through the indicated network access point. The order of these parameters in the characteristic tells in which order the ME MUST attempt to use the indicated proxies and network access points to contact the application, with the first parameter being the first one to be used. If access is not possible using an indicated proxy or network access point, the ME MUST attempt access according to the next included parameter. The parameters in the APPLICATION characteristic override the information given in the ACCESS characteristics (see 4.9.1.2).

If the APPLICATION characteristic does not include any TO-PROXY and TO-NAPID parameters, the application MUST be accessed according to the ACCESS characteristics that are present. If no ACCESS characteristics are included in the provisioning document, the ME MUST do the access using the proxies or network access points in the provisioning document, provided that the ME is able to use them and they are available according to the included VALIDITY and BOOTSTRAP characteristics.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

5. Provisioning Document Interaction

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

5.1 Implicit priority

The device (e.g. browser) might read connectivity configurations from several sources, for example from a smart card and from the device memory. The smart card 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 a smart card [PROVSC]
    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 provisioning documents added later to the device. If the device has auxiliary provisioning mechanisms (e.g. DHCP) then these have lower priority than provisioning documents pre-configured or added to the device. For example, the provisioning of DNS connectivity information from a [PROVCONT] compliant provisioning document has higher priority than DNS connectivity information from a DHCP server.

5.2 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 provisioning 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.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

6. 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].

6.1 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`.

6.2 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.`

6.3 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.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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 provisioning 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.

6.4 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

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

7. 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.

7.1 GSM/UMTS

The following selection process SHOULD be followed by the ME:

1) Search for bootstrap information in smart card, if no information is found then continue. Predefined bootstrap on the smart card has the highest priority. Priorities between SIM, RUIM, UICC 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/UMTS 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 provisioning 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/UMTS USSD it is possible to use the WCMP Echo Request message to find out whether the client supports WAP over GSM/UMTS 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/UMTS USSD.

3) Otherwise the WAP Proxy knows that GSM/UMTS USSD is not available. It can then let the TPS proceed with the bootstrap process via GSM/UMTS SMS.

7.2 CDMA

The following selection process SHOULD be followed by the ME:

1) Search for bootstrap information in smart card, if no information is found then continue. Predefined bootstrap on the smart card has the highest priority. Priorities between RUIM, UICC and WIM are specified in the Smart Card Provisioning Specification [PROVSC].
2) Search for persistent bootstrap information in the device.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

8. Management of Multiple Contexts

A device may contain one or more configuration contexts of which one SHOULD 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 ensure that the user has ultimate control over configurations of his phone, assuming that the user interface of the device provides the necessary management tools.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
WAP-185-ProvUAB-20010314-a	2001-03-14	Approved

A.2 Draft/Candidate Version 1.1 History

Reference	Date	Sections	Description
Draft Versions OMA-WAP-ProvUAB-v1_1	14-Mar-2001		The initial approved version of this document.
	10-Apr-2002	all	New template. Editorial corrections.
	16-May-2002	4.5, A.4	Use of domain name as proxy address.
	16-May-2002	A.3	Fix SCR entry numbering
	10-Sep-2002	all	Switch to OMA Continued Work template
	18-Sep-2002		Editorial corrections
	19-Sep-2002	4.5	Improved phrasing
	19-Sep-2002	3.3, 4.6, 5.1, A.4	Integrated changes adding ACCESS characteristic
	29-Oct-2002		Updated after Architectural Consistency review.
	31-Oct-2002		Integrated CR-ProvUAB-20020523-Ericsson
	31-Oct-2002	4.10	Add section to address Architectural Consistency review comments.
	05-Oct-2002	3.2,3.3,4.1,A.4	Editorial corrections.
	13 Nov 2002	A.4	Address comments from followup Architectural Consistency review
Candidate Versions OMA-WAP-ProvUAB-v1_1	28 Apr 2005	8, B.7	Template update CR 2003-0093 incorporated.
Draft Versions OMA-WAP-ProvUAB-v1_1	10 Oct 2007	All	Updated with agreed CR OMA-DM-CP-2006-0006
Candidate Versions OMA-WAP-ProvUAB-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

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Appendix B. Static Conformance Requirements (Normative)

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

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

B.1. General User Agent Behaviour Features

Item	Function	Reference	Status	Requirement
ProvUAB-U-C-001	Support for the `wap-provisioningdoc`	**Error! Reference source not found.**	M	
ProvUAB-U-C-002	Support for Proxy Selection	**Error! Reference source not found.**	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	**Error! Reference source not found.**	O	
ProvUAB-U-C-004	Support for local bootstrap by WIM/SIM/UICC	7.1	O	
ProvUAB-U-C-005	Support for provisioning document conflict resolution.	5.2	M	
ProvUAB-U-C-006	Support for local bootstrap by WIM/RUIM/UICC	7.2	O	

B.2. Proxy Selection

Item	Function	Reference	Status	Requirement
ProvUAB-UPS-C-001	Support for authority match	6.1	O	
ProvUAB-UPS-C-002	Support for path match	6.2	O	
ProvUAB-UPS-C-003	Support for best match	6.3	O	

B.3. Conflict Resolution

Item	Function	Reference	Status	Requirement
ProvUAB-UCR-C-001	Redundant characteristics ignored	4.1	M	
ProvUAB-UCR-C-002	Redundant parameters ignored	4.1	M	
ProvUAB-UCR-C-003	Unknown characteristics ignored	4.1	M	
ProvUAB-UCR-C-004	Unknown parameters ignored	4.1	M	
ProvUAB-UCR-C-005	Unknown values ignored	4.1	M	
ProvUAB-UCR-C-006	Discard redundant NAP definitions but continue to process document	4.1	M	

B.4. Use of Provisioning Document Parameters

Item	Function	Reference	Status	Requirement
ProvUAB-UDP-C-001	Ignore NAP definition when bearer not supported	4.2	M	
ProvUAB-UDP-C-002	Ignore physical proxy definitions containing only unsupported	4.2	M	

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Item	Function	Reference	Status	Requirement
	protocols			
ProvUAB-UDP-C-003	Ignore physical proxy definitions without a valid NAP	4.2	M	
ProvUAB-UDP-C-004	Ignore logical proxy definitions without a valid physical proxy.	4.2	M	
ProvUAB-UDP-C-005	Support for PXADDR-FQDN	4.5	O	
ProvUAB-UDP-C-006	Use of PORT characteristic	4.6	M	
ProvUAB-UDP-C-007	Usage of parm PXAUTH-ID	4.7	O	
ProvUAB-UDP-C-008	Usage of parm CLIENT-ID	4.7	O	
ProvUAB-UDP-C-009	Handling of missing authentication credentials	4.8	O	
ProvUAB-UDP-C-010	Support for interpreting ACCESS characteristic	4.9	M	
ProvUAB-UDP-C-011	Support for Granting Access condition	4.9.1	M	
ProvUAB-UDP-C-012	Support for multiple access-rule parameters	4.9.1.1	M	
ProvUAB-UDP-C-013	Support for Access Selection mechanism	4.9.1.2	M	
ProvUAB-UDP-C-014	Support for multiple access-result parameters	4.9.1.3	M	
ProvUAB-UDP-C-015	Co-ordinating Access Selection and Proxy Selection	4.9.2	M	
ProvUAB-UDP-C-016	Interpretation of APPLICATION chracteristics	4.10	O	

B.5. Error Handling

Item	Function	Reference	Status	Requirement
ProvUAB-UEH-C-001	Ignore unknown tags and attributes in provisioning document	4.3	O	
ProvUAB-UEH-C-002	Ignore document with unsupported major version number	4.3	M	
ProvUAB-UEH-C-003	Ignore parameters and values that are unrecognised	4.3	O	
ProvUAB-UEH-C-004	Ignore corrupt document	4.3	O	
ProvUAB-UEH-C-005	Look for a valid document when current one is invalid	4.3	O	

B.6. GSM Bootstrap

Item	Function	Reference	Status	Requirement
ProvUAB-UGSM-C-001	Support for bootstrap in GSM	7.1	O	ProvUAB-UGSM-C-002 AND ProvUAB-UGSM-C-003 AND ProvUAB-UGSM-C-004
ProvUAB-UGSM-C-002	WIM/SIM/UICC has higher priority than Cell Broadcast	7.1	O	
ProvUAB-UGSM-C-003	Cell Broadcast has higher priority than SMS/USSD	7.1	O	
ProvUAB-UGSM-C-004	SMS and USSD have equal priority	7.1	O	
ProvUAB-UGSM-C-005	Support for Cell Broadcast in GSM	7.1	O	ProvUAB-UGSM-C-006

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Item	Function	Reference	Status	Requirement
ProvUAB-UGSM-C-006	GSM Cell Broadcast channel monitored when WAP initialised	7.1	O	

B.7. Multiple Context Management

Item	Function	Reference	Status	Requirement
ProvUAB-UCM-C-001	Support for Privileged Configuration Context	**Error! Reference source not found.**	O	
ProvUAB-UCM-C-002	User can make additions to Privileged configuration Context	**Error! Reference source not found.**	O	
ProvUAB-UCM-C-003	NETWPIN bootstrap restricted to single context	**Error! Reference source not found.**	O	
ProvUAB-UCM-C-004	Support for multiple bootstraps using a User PIN method	**Error! Reference source not found.**	O	
ProvUAB-UCM-C-005	Support for short lived PIN	**Error! Reference source not found.**	O	

B.8. CDMA Bootstrap

Item	Function	Reference	Status	Requirement
ProvUAB-UCDMA-C-001	Support for bootstrap in CDMA	7.1	O	ProvUAB-UCDMA-C-002
ProvUAB-UCDMA-C-002	WIM/RUIM/UICC has highest priority	7.2	O	

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.