Provisioning Bootstrap

Candidate Version 1.1 – 28 Apr 2005

Open Mobile Alliance

OMA-WAP-ProvBoot-V1_1-20050428-C

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 Open Mobile Alliance 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 initially configured with connectivity and application access parameters. The provisioning process also includes subsequent updates of persistent information in WAP client devices as well as retrieval of management information stored on WAP client devices.

The term covers both OTA provisioning and provisioning by means of, e.g., SIM cards. This specification defines a part of the provisioning process, namely, the bootstrap process, which is an OTA mechanism used to initially provision unconfigured WAP clients when, e.g., a SIM card containing WAP provisioning information is not available.

2. References

2.1. Normative References

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

[GSM03.38] "Alphabets and Language Specific Information", ETSI, URL: http://www.etsi.org/

[GSM11.11] Digital cellular Telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11 version 7.2.0 Release 1998)

[HMAC] "HMAC: Keyed-Hashing for Message Authentication", Krawczyk, H., Bellare, M., and Canetti, R., RFC 2104, February 1997. URL: ftp://ftp.isi.edu/in-notes/rfc2104.txt

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

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

[PROVSC] "OMA Smart Card Provisioning Specification", Open Mobile Alliance ™, OMA-WAP-PROVSC-v1_1, URL: http://www.openmobilealliance.org

[PROVUAB] "OMA Provisioning User Agent Behaviour Specification", Open Mobile Alliance ™, OMA-WAP-PROVUAB-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

[SHA] "Secure Hash Standard", NIST FIPS PUB 180-1, National Institute of Standards and Technology, U.S. Department of Commerce, DRAFT, May 1994.

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

[TIA/EIA-136-720-A] "Over-the-Air Activation Teleservice (OATS)", TIA/EIA, TIA/EIA-136-720-A

[TIA/EIA-637-A] "Short Message Service for Spread Spectrum Systems", TIA/EIA, TIA/EIA-637-A

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

[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

[WTLS] "Wireless Transport Layer Security", WAP Forum ™, WAP-261-WTLS, URL: http://www.openmobilealliance.org

2.2. Informative References

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

[WAPARCH] "WAP Architecture Specification", WAP Forum ™, WAP-210-WAPArch, 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,” are normative, unless they are explicitly indicated to be informative.

3.2. Definitions

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

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.
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.
Privileged Configuration Context	A privileged configuration context is a special context in which it is possible to define the number of additional configuration contexts allowed. Not all WAP service providers are, however, allowed to bootstrap the privileged context.
Provisioned state	The state in which the ME has obtained connectivity information extending its access capabilities for content, applications or continuous provisioning. This state is reached when the bootstrap process has provided access to generic proxies, or the continuous provisioning process has been performed.
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.

3.3. Abbreviations

CB	Cell Broadcast
DCS	Data Coding Scheme
ESN	Electronic Serial Number
GHOST	GSM Hosted Teleservice
GSM	Global System for Mobile Communication
GUTS	General UDP Transport Service
HMAC	Hashed Message Authentication Code
ID	Identifier
IMSI	International Mobile Subscriber Identifier
MAC	Message Authentication Code
ME	Mobile Equipment
MIME	Multipurpose Internet Mail Extensions
MSISDN	Mobile Station Integrated Services Directory Number
NAM	Number Assignment Module
NAP	Network Access Point
OTA	Over The Air
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
SEC	Security Method
SHA	Security Hashing Algorithm
SIM	Subscriber Identity Module
SMS	Short Message Service
SPC	Service Programming Code
SSD	Shared Secret Data
TPS	Trusted Provisioning Server
UDP	User Datagram Protocol
URL	Uniform Resource Locator
USSD	Unstructured Supplementary Service Data
WAP	Wireless Application Protocol
WBXML	Wireless Binary Extensible Markup Language
WDP	Wireless Datagram Protocol
WIM	Wireless Identity Module
WTLS	Wireless Transport Layer Security

4. Bootstrap Introduction

The bootstrap process is performed when an unconfigured configuration context within the ME must be provisioned with WAP connectivity or application access information, see [PROVARCH]. Since an unconfigured configuration context does not have sufficient information to establish a WAP connection to the infrastructure the bootstrap process will, to some extent, rely on the mechanisms available in the underlying network technology.

The bootstrap process establishes a basic relationship between the device and the network, i.e. an initial set of configuration information. This information, at a minimum a network access point and a proxy, and usually a content location (the Trusted Provisioning Server), specifies an access method to WAP resources. The bootstrap process is in particular able to specify, using a Trusted Proxy, an access path to a Trusted Provisioning Server (TPS).

It is possible to define access to generic WAP proxies in the bootstrap process. It is even possible to omit the definition of a TPS if there is no intention to perform continuous provisioning over the air.

The intended result of this bootstrap process is that the device has a trusted point of configuration, i.e. a TPS. This initial configuration can be leveraged by the continuous provisioning mechanism. Thanks to the separation of the bootstrap and the continuous provisioning the former is allowed to be network and bearer specific while the latter is generic.

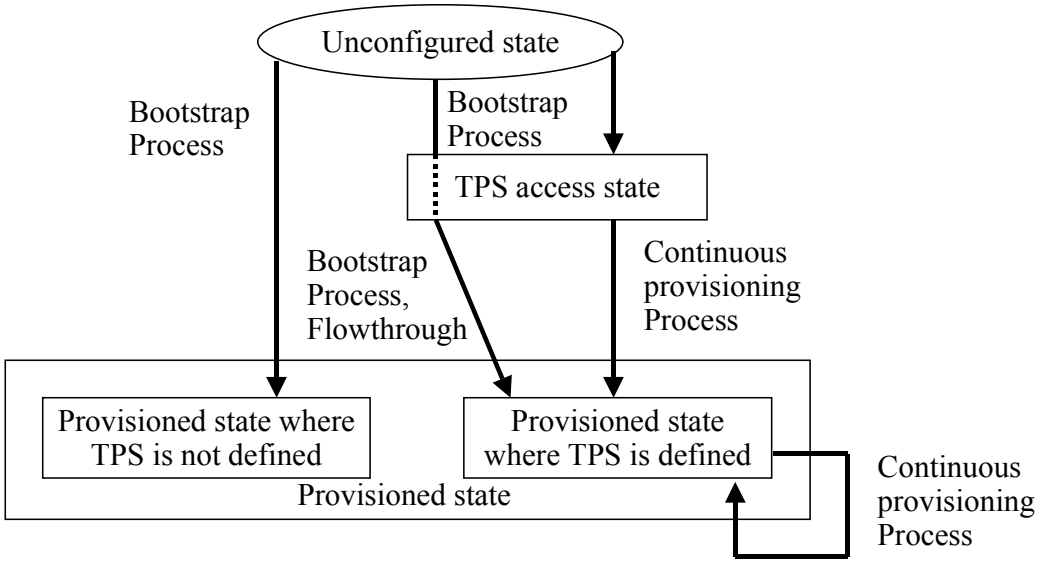

Fig. 1 - The configuration context normally is in the provisioned state. The two boxes for the provisioned state show that it is possible to do continuous provisioning only if a Trusted Proxy and a Provisioning URL are defined.

4.1. Bootstrap of Configuration Context

The PROVURL parameter (including host and path) of the bootstrap document defines a location of a Trusted Provisioning Server. Each PROVURL MUST be unique within the device, and does thus identify a separate configuration context. The device MUST thus either automatically discard redundant bootstrap messages, or allow the user to manually select a handling.

An exception from the above rule is if a bootstrap is done without a PROVURL definition, i.e. missing or empty definition. Multiple bootstraps without a PROVURL definition MAY be accepted as unique and separate, and MUST then create independent configuration contexts.

5. The Bootstrap Process

5.1. OTA Mechanism

The OTA bootstrap process MUST be initiated by a dedicated server that sends a bootstrap document via WAP connectionless push [WAPPUSH] with the default push port, the default application ID and the provisioning MIME-type (`application/vnd.wap.connectivity-wbxml`) to the ME. This ensures that the bootstrap mechanism is able to work on most bearers that support network initiated communication using [WAPWDP].

5.2. Security Mechanisms

Since the bootstrap process enables an infrastructure entity to configure a configuration context of the ME, it is important that the following security requirements are met:

1. The server that is initiating the bootstrap process MUST be authenticated.
2. The client for which the bootstrap process is targeted MUST be authenticated using network level validation mechanisms in networks where such services are available.

It is assumed that the underlying network technology provides a means for identifying and (maybe only implicitly) authenticating the client. For GSM, for example, the routing of SMS based on the MSISDN of the client provides an implicit authentication of the client.

For the server authentication, two methods are considered as described below. In some situations these methods may not apply, due to the implicit security of the underlying network mechanism.

The definition of a Privileged Configuration Context allows to assign a higher level of security to that context than to the optional other contexts.

5.2.1. The Generic Security Mechanism

The generic security mechanisms are intended to be available for all bearers. The generic security mechanism MUST be supported in all cases, except when the underlying network provides a security mechanism with similar protective characteristics. In some cases the generic mechanisms might not apply due to the implicit security of the bearer network, in all other cases the methods USERPINMAC and USERNETWPIN MUST be supported. The generic mechanisms are either based on a secret that is shared between the ME and the correct sender of the bootstrap document or an out-of-band mechanism for delivering some authentication information. What constitutes the shared secret depends on the underlying network technology.

Bootstrap security by means of a shared secret

In order to provide security by means of a shared secret, security information MUST be provided with the bootstrap document. The security information MUST include the MAC and the security method (SEC), which are transported as parameters to the media type in the content type header (see [PROVCONT]). If the SEC takes the value USERPIN, the shared secret is based on a user PIN. If the SEC takes the value NETWPIN, the shared secret is based on a network specific shared secret. Finally, if the SEC is USERNETWPIN, the shared secret is a network specific shared secret appended with a user PIN.

When presented to the user as well as when used as input to the MAC calculation, the user PIN MUST be a string of ASCII encoded decimal digits (i.e. octets with hexadecimal values 30 to 39). The format of the network specific shared secret that is used as input to the MAC calculation is dependent on the network technology. The format to be used within each network technology is defined in each of the network specific adaptations in chapter 6.

The MAC is calculated in the following way:

First, the bootstrap document is encoded in the WBXML format [WBXML]. The so encoded document and the shared secret are then input as the data and key, respectively, for the HMAC calculation [HMAC], based on the SHA-1 algorithm [SHA], as defined in the WTLS specification [WTLS]. The output of the HMAC (M = HMAC-SHA(K, A)) calculation is encoded as

a string of hexadecimal digits where each pair of consecutive digits represent a byte. The hexadecimal encoded output from the HMAC calculation is then included in the security information.

This calculation is repeated in the ME when checking the validity of the MAC.

Bootstrap security by means of an out-of-band delivery of the MAC authentication information

In order to provide security by means of an out-of-band delivery of authentication information (e.g. PIN includes the MAC), certain security information MUST be provided with the bootstrap document. The security information MUST include the security method, which is given in the SEC connectivity media type parameter (see [PROVCONT]), but MUST NOT include the MAC. Instead, the user receives a PIN inclusive of the MAC from the generator of the bootstrap document by some out-of-bands mechanism. The PIN is then used to check the validity of the bootstrap document. The PIN MUST consist of a 2*L decimal digits (where L is a number bigger than 4), and MUST be generated as follows:

1) Let A be the WBXML encoded bootstrap document.
2) Generate a random string K of ASCII encoded decimal digits (i.e. octets with hexadecimal values 30 to 39) with length L.
3) Calculate the array of octets M = HMAC-SHA(K, A).
4) Generate a string m of length L from M according to m(i) = M(i) mod 10 + 48, where i refers to the individual elements of the string m and array M, respectively.
5) Generate the PIN code C as a concatenation C = K || m.

When the ME receives a bootstrap document with the SEC set to USERPINMAC, the process is repeated:

1) Let A be the WBXML encoded bootstrap document.
2) Retrieve the string K from the first half of the PIN code C = K || m, which has the length 2*L.
3) Calculate the array of octets M' as above.
4) Generate a string m' as above.

If m' and m are identical the bootstrap document can be accepted.

5.2.2. Additional Bearer Specific Security Mechanisms

Some bearers may require support for special security mechanisms in addition to the generic security mechanism. This could, for example, be the case if the shared secret available for the generic security mechanism is not considered sufficiently safe. Specification of such additional mechanisms is relegated to the next chapter.

6. Network Specific Adaptations

6.1. Adaptation to GSM

In GSM, if USERNETWPIN or NETWPIN is used, the IMSI MUST be used as the network specific shared secret. When used as input to the MAC calculation, the IMSI MUST be on semi-octet representation as defined in [GSM11.11]. The length indicator byte and possible unused bytes (i.e. the IMSI is less than 15 digits) MUST NOT be used. If the IMSI consists of an even number of digits the filler 0xF MUST be inserted.

6.1.1. SIM

Bootstrap data stored on the SIM or SIM/WIM card, [PROVSC], has the highest priority (see [PROVUAB]). If data is found on the SIM or SIM/WIM card no over the air bootstrap procedure is valid for that Configuration Context. Update of bootstrap data can be done only using out of band methods, i.e. smart card specific methods (for example a non-WAP over the air configuration method).

The SIM or SIM/WIM may store data of a Privileged Configuration Context.

If the device claims to support WIM functionality it MUST also support reading of connectivity parameters from the WIM card and the SIM card.

6.1.2. Cell Broadcast

The mechanism for Cell Broadcast bootstrap is network initiated. No user PIN or shared secret needs to be used as the same bootstrap message is delivered to all mobiles within a particular area.

The security mechanism that protects the device from arbitrary configuration messages is based on the sole use of broadcast channel 421. The device SHALL only accept bootstrap messages on this broadcast channel. However, the device cannot assume that the channel only contains bootstrap messages. It is recommended that network providers restrict other traffic than bootstrap messages on this particular channel, or ensures that only authorised bootstrap messages are sent on the channel.

A bootstrap message is addressed to a particular group of mobiles, i.e. the mobiles of a carrier, using the network code. The SIM card, and thus device, has a network code as part of the IMSI parameter. This network code is compared to the network code provided by the network and a parameter in the provisioning content type.

The mechanism for approving a bootstrap message based on a Network Code match is defined as follows. There are three network codes:

- A provisioning Network Code as available from the bootstrap document
- A SIM Network Code (the Network Code = Mobile Country Code & Mobile Network Code) available from the IMSI on the SIM
- A System Network Code (Mobile Country Code and Mobile Network Code as specified in the system information messages transmitted on the broadcast control channel)

The System Network Code, Provisioning Network Code and SIM Network Code MUST be equal in order for the message to be accepted as valid bootstrap information.

Cell Broadcast may transmit data for a Privileged Configuration Context.

If the device supports any kind of SMS Cell Broadcast, for example text SMS-CB, then it MUST also support WAP bootstrap over SMS-CB.

Guidelines for Network Management

For the use of CB, the following configurations of CB in the network have to be provided

- The CB parameter Geographical Scope MUST be coded to "PLMN wide validity" implying automatically the coding of the CB parameter Display mode as “Normal Display”.

- The CB Parameter Update Number has a value of 0 when the bootstrap parameters are broadcast the first time. If the bootstrap parameters will change in future, the bootstrap message is appropriately adapted by the operator, i.e. a normal change procedure is invoked at the CBC (Cell Broadcast Centre), leading to an update of the content of the bootstrap message and to an automatic increment of the Update Number. A new Update Number can be taken by the MS as an indication of a change of the bootstrap parameters and trigger a verification process of the parameter set. The Update Number is incremented cyclically between 0 and 15.

- The CB parameter Message Identifier (MI) indicates the logical CB channel on which a CB message is broadcast. There will be one single WAP-CB-Channel carrying the bootstrap information: MI = 421.

- CB scheduling messages MUST be used as follows: If the duration of the schedule period is assumed to be one minute, i.e. 32 CB messages can be broadcast within one schedule period, there are 32 CB message slots. The first CB message slot carries the *scheduled* schedule message (CB message slot 0). CB messages that are to be broadcast (e.g. the bootstrap message) are spread over the CB message slots according to their repetition rate. If there is a free CB message slot without any CB message to be broadcast, the network SHALL send *unscheduled* schedule messages in this slots, i.e. schedule messages that are not broadcast in CB message slot 0, but in any other CB message slot.

6.1.3. SMS

The bootstrap mechanism when using SMS is network initiated. Bootstrapping over SMS MUST use one of the generic security mechanisms. To this end, the network specific shared secret is the IMSI as specified in section 6.1.

This mechanism MUST NOT be used to transfer bootstrap data to a Privileged Configuration Context, unless network shared secret is used in combination with other security mechanisms, i.e. USERNETWPIN. Note, that the privileged configuration context SHOULD be supported as per [ProvUAB].

If the device supports any kind of SMS Point to Point, for example mobile terminated text SMS, then it MUST also support WAP bootstrap over SMS.

6.1.4. USSD

The bootstrap adaptation using GSM USSD is network initiated. Bootstrapping over USSD MUST use one of the generic security mechanisms. To this end, the network specific shared secret is the semi-octet representation of the IMSI.

All WAP messages, including the pushed provisioning message, are distinguished by a reserved DCS (Data Coding Scheme, [GSM03.38]) for WAP.

USSD MUST NOT be used to transfer bootstrap data to a Privileged Configuration Context, unless the network shared secret is used in combination with other security mechanisms, i.e. USERNETWPIN. Note, that the privileged configuration context SHOULD be supported as per [ProvUAB].

6.1.5. User Agent Behaviour

All configuration data, including the bootstrap data, is tied to a specific identity of the SIM, i.e. the IMSI. If a new (different) SIM is inserted the device should keep the original configuration private (not visible). The phone might store multiple configurations, each tied to a particular IMSI.

When receiving a bootstrap document, the ME MUST validate the document (where applicable) using the prescribed methods. Only bootstrap documents that are properly authenticated SHALL be accepted.

The bootstrap over point to point bearers such as GSM SMS and GSM USSD is a one-time event per configuration context. Within a configuration context, the bootstrap process cannot be re-performed unless the context is reset (using an out of band method). The bootstrap data set established over broadcast bearers (e.g. Cell Broadcast) can be updated (including a complete reset of the configuration context) using the same bearer.

The ME MAY provide a capability to reset a configuration context to the unconfigured state, thereby allowing the bootstrap process to be reinitiated for that context.

6.2. Adaptation to TDMA (TIA/EIA-136)

6.2.1. GUTS

The bootstrap mechanism when using GUTS is network initiated. Bootstrapping over GUTS MUST use the generic security mechanism based on bootstrap security by means of a shared secret.

For the mobile equipment (ME) to authenticate the originator of the bootstrap message, the following method SHALL be used:

- The generator of the bootstrap message SHALL attach a SEC attribute.
- The network specific shared secret data SHALL be set to the value of the Shared Secret Data - Subsidy (SSD_S) parameter stored by both the ME and the generator of the bootstrap document, concatenated with the 32 bit ESN (network specific shared secret data = SSD_S || ESN). The 64-bit SSD_S parameter is the same parameter that is used for authenticating an activation centre for NAM updating as defined in TIA/EIA-136-720-A, sections 7.110 and 5.3. Note that the bootstrap method described herein is used in lieu of the out of band method described in TIA/EIA-136-720-A. The ESN parameter is as defined in section 4.2.1 of TIA/EIA-136-005-A.
- The originator of the bootstrap message SHALL calculate the HMAC using the network specific shared secret data (SSD_S || ESN) as the key for the SHA-1 algorithm as specified in section 6.2.1. This HMAC calculation will be used as the MAC in validation of the bootstrap document.
- The ME SHALL use the same calculation to authenticate the originator of the bootstrap message based on the MAC.

Only the network shared secret method (SEC=NETWPIN) shall be used to bootstrap the Privileged Configuration Context.

6.2.2. User Agent Behaviour

All Configuration Contexts, including the bootstrap data, are tied to a specific NAM (Number Assignment Module) of the ME. The ME MAY store multiple configuration contexts, privileged or otherwise, per NAM. Each Configuration Context is specific to a certain NAM. When a configuration document is delivered to the ME, the configuration context(s) specified in the document SHALL apply only to the NAM that is active at the time of delivery.

The ME SHALL authenticate the originator of the bootstrap provisioning document using the procedures specified in section 6.2.1. Only the network shared secret method (SEC=NETWPIN) shall be used to bootstrap the Privileged Configuration Context. Note, that the privileged configuration context MUST be supported as per [ProvUAB]. In the event of an authentication failure, the mobile SHALL NOT update its memory with the configuration data that was sent in the bootstrap message.

The bootstrap over point to point bearers such as GUTS is a one-time event per configuration context. Within a configuration context, the bootstrap process cannot be re-performed unless the context is reset (using an out of band method).

6.3. Adaptation to CDMA

6.3.1. SMS

The bootstrap protocol MAY be delivered to the ME using various transport mechanisms including IS95B and CDMA2000. These mechanisms SHALL include the use of mobile-terminated SMS as per [TIA/EIA-637-A] on the paging channel. The bootstrap message includes a MAC, which is calculated based on shared secret data (SSD) and is included in the bootstrap message as described in the Generic Security Mechanism section. If a network specific shared secret is used, the network specific shared secret MUST be in binary format when used as input to the MAC calculation.

For the mobile station to authenticate to the TPS the following methods SHALL be used. The SSD SHALL be a combination of known ESN and SPC values. More specifically, the SSD is the 32-bit ESN appended with the 24-bit SPC (service

programming code), or SSD entered by the user. The TPS SHALL employ a hash algorithm to transform the ESN and SPC values into an HMAC calculation as per section 6.2.1, which will be included in the bootstrap data and validated by the client.

Only the methods NETWPIN and USERNETWPIN are allowed to be used to bootstrap the privileged configuration context.

This mechanism may transmit data for a Privileged Configuration Context if network shared secret is used.

6.3.2. User Agent Behaviour

All configuration contexts, including the bootstrap data, are tied to a specific NAM (Number Assignment Module) of the ME. The phone MAY store multiple configuration contexts, privileged or otherwise, per NAM. Each configuration context is specific to a certain NAM.

The ME SHALL check the validity of the bootstrap document using the authentication procedures specified in section 6.2.1. Only NETWPIN or USERNETWPIN are allowed to bootstrap the privileged context. Note, that the privileged configuration context SHOULD be supported as per [ProvUAB]. If SEC consists of USERNETWPIN, the user PIN is also validated. In the event of an authentication failure, the mobile SHALL NOT update its memory with TPS configuration data.

The ME MAY provide a capability to reset a configuration context to the unconfigured state, thereby allowing the bootstrap process to be reinitiated for that context.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version –or- No previous version within OMA

A.2 Draft/Candidate Version 1.1 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-WAP-ProvBoot	17-Sept-2001	All	The initial draft version of this document. - Class 0
Candidate Versions OMA-WAP-ProvBoot-v1_1	12-Nov-2002	n/a	ACG review updates - Class 3
	28 Apr 2005	6.1.3, 6.1.4, 6.2.2, 6.3.2, Appendix B	Template update CR 2003-0093 incorporated

Appendix B. Static Conformance Requirements (Normative)

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

B.1 Preconditions

Item	Function	Reference	Status	Requirement
ProvBoot-BPC-C-001	The device supports WIM in the scope of WAP Class Conformance.		O	ProvBoot-B-C-002
ProvBoot-BPC-C-002	The device supports the GSM SMS bearer in some form, i.e. for example point to point Mobile Terminated text SMS.		O	ProvBoot-BGSM-C-004
ProvBoot-BPC-C-003	The device supports the broadcast bearer GSM CB-SMS in some form, i.e. for example text CB-SMS.		O	ProvBoot-BGSM-C-003

B.2 General Bootstrap Feature

Item	Function	Reference	Status	Requirement
ProvBoot-B-C-001	Support for the WAP-PROVISIONINGDOC	5.1	M	ProvBoot-B-C-002 OR ProvBoot-B-C-003 OR ProvBoot-B-C-004 OR ProvBoot-B-C-005
ProvBoot-B-C-002	Support for WAP-PROVISIONINGDOC read from WIM/SIM	5	O	ProvBoot-BGSM-C-001 AND ProvBoot-BGSM-C-002
ProvBoot-B-C-003	Support for WAP-PROVISIONINGDOC received Over The Air using a Point to Point mechanism	5	O	ProvBoot-B-C-006 AND (ProvBoot-BCT-C-001 OR ProvBoot-BCT-C-002 OR ProvBoot-BCT-C-003 OR ProvBoot-BCT-C-004)
ProvBoot-B-C-004	Support for WAP-PROVISIONINGDOC received Over The Air using a Broadcast mechanism	5	O	
ProvBoot-B-C-005	Support for WAP-PROVISIONINGDOC read from the device (pre-configured bootstrap)	5	O	

Item	Function	Reference	Status	Requirement
ProvBoot-B-C-006	Support for WAP-PROVISIONINGDOC generic security mechanism	5.2.1	O	ProvBoot-BSF-C-003 AND ProvBoot-BSF-C-004
ProvBoot-B-C-007	Support for multiple configuration context	4.1	O	ProvBoot-B-C-009
ProvBoot-B-C-008	Each PROVURL is unique within the device, and identifies a separate configuration context.	4.1	M	
ProvBoot-B-C-009	Support for multiple bootstraps without a PROVURL definition	4.1	O	ProvBoot-B-C-010
ProvBoot-B-C-010	In case multiple bootstraps without a PROVURL definition are accepted then they create independent configuration contexts.	4.1	O	
ProvBoot-B-C-011	Support for WAP connectionless push for initiation of the OTA bootstrap process	5.1	M	

B.2.1 Bearer Support

Item	Function	Reference	Status	Requirement
ProvBoot-BCT-C-001	Support for the GSM	6.1	O	ProvBoot-BGSM-C-001 OR ProvBoot-BGSM-C-002 OR ProvBoot-BGSM-C-003 OR ProvBoot-BGSM-C-004 OR ProvBoot-BGSM-C-005
ProvBoot-BCT-C-002	Support for - IS-95-CDMA	6.3	O	ProvBoot-BCDMA-C-001
ProvBoot-BCT-C-003	Support for IS-136-TDMA	6.2	O	ProvBoot-BTDMA-C-001
ProvBoot-BCT-C-004	Support for Generic Over The Air Mechanism	5.2.1	O	

B.3 GSM Features

Item	Function	Reference	Status	Requirement
ProvBoot-BGSM-C-001	Support for WAP-PROVISIONINGDOC read from WIM	6.1.1	O	ProvBoot-BGSM-C-014

Item	Function	Reference	Status	Requirement
ProvBoot-BGSM-C-002	Support for WAP-PROVISIONINGDOC read from SIM	6.1.1	O	ProvBoot-BGSM-C-014
ProvBoot-BGSM-C-003	Support for WAP-PROVISIONINGDOC received by Cell Broadcast	6.1.2	O	ProvBoot-BGSM-C-009 AND ProvBoot-BGSM-C-010 AND ProvBoot-BGSM-C-011 AND ProvBoot-BGSM-C-014
ProvBoot-BGSM-C-004	Support for WAP-PROVISIONINGDOC received over SMS bearer	6.1.3	O	ProvBoot-BGSM-C-006 AND ProvBoot-BGSM-C-007 AND ProvBoot-BGSM-C-008 AND ProvBoot-B-C-003 AND ProvBoot-BGSM-C-014
ProvBoot-BGSM-C-005	Support for WAP-PROVISIONINGDOC received over USSD bearer	6.1.4	O	ProvBoot-BGSM-C-006 AND ProvBoot-BGSM-C-007 AND ProvBoot-BGSM-C-008 AND ProvBoot-B-C-003 AND ProvBoot-BGSM-C-014
ProvBoot-BGSM-C-006	Validate the bootstrap document using generic security mechanism.	6.1.5	O	
ProvBoot-BGSM-C-007	Accept only bootstrap documents that are authenticated.	6.1.5	O	
ProvBoot-BGSM-C-008	Privileged context accepted only if authenticated using USERNETWPIN	6.1.3, 6.1.4	O	
ProvBoot-BGSM-C-009	The CB parameter Geographical Scope encoded as "PLMN wide validity"	6.1.2	O	
ProvBoot-BGSM-C-010	The System Network Code, Provisioning Network Code and SIM Network Code are equal in order for the message to be accepted as valid bootstrap information.	6.1.2	O	
ProvBoot-BGSM-C-011	The channel 421 is used for bootstrap messages.	6.1.2	O	
ProvBoot-BGSM-C-012	Support for network specific shared secret	6	O	ProvBoot-BGSM-C-013

Item	Function	Reference	Status	Requirement
ProvBoot-BGSM-C-013	The network specific shared secret is the IMSI	6.1.1	O	
ProvBoot-BGSM-C-014	Support for privileged configuration context	6.1.3, 6.1.4	O	

B.4 IS-95-CDMA Features

Item	Function	Reference	Status	Requirement
ProvBoot-BCDMA-C-001	Support for WAP-PROVISIONINGDOC received over SMS bearer	6.3	O	ProvBoot-B-C-003 AND ProvBoot-BCDMA-C-006
ProvBoot-BCDMA-C-002	Validate the bootstrap document using generic security mechanism.	6.3	O	
ProvBoot-BCDMA-C-003	Accept only bootstrap documents that are authenticated.	6.3	O	
ProvBoot-BCDMA-C-004	Support for network specific shared secret	6.3	O	ProvBoot-BCDMA-C-005
ProvBoot-BCDMA-C-005	The network specific shared secret is the SSD	6.3	O	
ProvBoot-BCDMA-C-006	Support for privileged configuration context	6.3.2	O	ProvBoot-BSF-C-001 OR ProvBoot-BSF-C-003

B.5 IS-136-TDMA Features

Item	Function	Reference	Status	Requirement
ProvBoot-BTDMA-C-001	Support for WAP-PROVISIONINGDOC received over the GUTS bearer	6.2.1	O	ProvBoot-B-C-003 AND ProvBoot-BTDMA-C-002 AND ProvBoot-BTDMA-C-003 AND ProvBoot-BTDMA-C-004 AND ProvBoot-BTDMA-C-005 AND ProvBoot-BSF-C-001
ProvBoot-BTDMA-C-002	Bootstrap message impacts only active NAM	6.2.2	O	

Item	Function	Reference	Status	Requirement
ProvBoot-BTDMA-C-003	Discard bootstrap message if generic security mechanism fails.	6.2.2	O	
ProvBoot-BTDMA-C-004	NETWPIN consists of concatenated SSD_S and ESN	6.2.1	O	
ProvBoot-BTDMA-C-005	Support for privileged configuration context	6.2.2	O	ProvBoot-BSF-C-001

B.6 Generic Security Features

Item	Function	Reference	Status	Requirement
ProvBoot-BSF-C-001	Support for NETWPIN	5.2.1	O	
ProvBoot-BSF-C-002	Support for USERPIN	5.2.1	O	
ProvBoot-BSF-C-003	Support for USERNETWPIN	5.2.1	O	
ProvBoot-BSF-C-004	Support for USERPINMAC	5.2.1	O	