



OMA Device Management Bootstrap

Candidate Version 1.3 – 09 Oct 2012

Open Mobile Alliance
OMA-TS-DM_Bootstrap-V1_3-20121009-C

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

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

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

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

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

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

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

1. SCOPE	5
2. REFERENCES	6
2.1 NORMATIVE REFERENCES	6
2.2 INFORMATIVE REFERENCES	7
3. TERMINOLOGY AND CONVENTIONS	8
3.1 CONVENTIONS	8
3.2 DEFINITIONS	8
3.3 ABBREVIATIONS	8
4. INTRODUCTION	9
5. BOOTSTRAPPING	10
5.1 BOOTSTRAP SCENARIOS	10
5.1.1 Requirements	10
5.1.2 Solutions	10
5.2 OTA BOOTSTRAP PACKAGE DELIVERY (INFORMATIVE)	14
5.3 BOOTSTRAP PROFILES	14
5.4 OMA CLIENT PROVISIONING PROFILE	15
5.4.1 Transports	15
5.4.2 Mapping Characteristic Data to the Management Tree.....	15
5.4.3 Management Object Location in the Management Tree.....	16
5.4.4 Management Object Access Rights	16
5.4.5 Special Behaviors - Smart Card Provisioning.....	16
5.4.6 Device Management, Access Point and Proxy Information.....	16
5.4.7 Other Client Provisioning information.....	16
5.5 OMA DEVICE MANAGEMENT PROFILE	16
5.5.1 Transport.....	16
5.5.2 Management tree ACL and bootstrap	17
5.5.3 Management Object Access Rights	17
5.5.4 Bootstrap Message Content	17
5.5.5 Processing of the Bootstrap.....	17
5.5.6 Smartcard.....	18
5.5.7 Bootstrap via HTTPS Get	19
6. BOOTSTRAP CONFIG MO	20
6.1 INTRODUCTION	20
6.2 GRAPHICAL REPRESENTATION (INFORMATIVE)	20
6.3 NODE DESCRIPTIONS	20
APPENDIX A. (INFORMATIVE)	23
A.1 APPROVED VERSION HISTORY	23
A.2 DRAFT/CANDIDATE VERSION 1.3 HISTORY	23
APPENDIX B. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE)	25
B.1 SCR FOR BOOTSTRAP CLIENT	25
B.2 SCR FOR BOOTSTRAP SERVER	26
B.3 SCR FOR BOOTSTRAP CONFIG MO	26
B.3.1 SCR for Bootstrap Config MO tree structure	26
B.3.2 SCR for Bootstrap Config MO functionality	26
B.3.3 SCR for DM System.....	27
APPENDIX C. GENERAL MAPPING	28
APPENDIX D. STORAGE OF DM BOOTSTRAP MESSAGE ON THE SMARTCARD (NORMATIVE)	29
D.1 FILE STRUCTURE	29
D.2 BOOTSTRAP MESSAGE ON SIM OR UICC ACTIVATED IN 2G MODE	30
D.2.1 Access to the file structure.....	30

D.2.2 Files Overview30

D.2.3 Access Method.....30

D.2.4 Access Conditions.....30

D.2.5 Requirements on the SIM or 2G UICC.....30

D.3 BOOTSTRAP MESSAGE ON UICC ACTIVATED IN 3G MODE.....31

D.3.1 Access to the file structure31

D.3.2 Files Overview31

D.3.3 Access Method.....31

D.3.4 Access Conditions.....31

D.3.5 Requirements on the 3G UICC31

D.4 FILES DESCRIPTION32

D.4.1 Object Directory File, EF ODF.....32

D.4.2 Bootstrap Data Object Directory File, EF DODF-bootstrap32

D.4.3 EF DM_Bootstrap.....34

APPENDIX E. DM BOOTSTRAP SERVER DISCOVERY (INFORMATIVE).....35

Figures

Figure 1: Customized bootstrap11

Figure 2: Bootstrap from smartcard.....12

Figure 3: Server initiated bootstrap13

Figure 4: Client initiated bootstrap.....14

Figure 5: Example Management Object and Name Identifiers15

Figure 6: Bootstrap Config MO.....20

Figure 7: File structure for Bootstrap Message on SIM smartcard or 2G UICC30

Figure 8: File structure for Bootstrap Message on 3G UICC31

Tables

Table 1: General Mapping28

1. Scope

This document defines the Bootstrap Process, the process of provisioning the DM Client to a state where it is able to initiate a management session to a new DM Server. DM Clients that have already been bootstrapped can be further bootstrapped to enable the DM Client to initiate a Management Session to new DM Servers or may be rebootstrapped to update existing accounts.

2. References

2.1 Normative References

[ACw7DM]	“OMA DM w7 Application Characteristic”. Working file in AC directory: URL:http://www.openmobilealliance.org/tech/omna/dm-ac/ac_w7_dm-v1_0.txt
[C.S0023-B_v1.0]	“Removable User Identity Module For Spread Spectrum Systems”, 3GPP2 C.S0023-B version 1.0, URL:http://www.3gpp2.org/Public_html/specs/C.S0023-B_v1.0_040426.pdf
[DMDICT]	“OMA Device Management Dictionary, Version 1.0”. Open Mobile Alliance™. OMA-SUP-DM_Dictionary-v1_0. URL:http://www.openmobilealliance.org
[DMSecurity]	“OMA Device Management Security, Version 1.2”. Open Mobile Alliance™. OMA-TS-DM_Security-V1_2. URL:http://www.openmobilealliance.org
[DMSTDOBJ]	“OMA Device Management Standardized Objects, Version 1.2”. Open Mobile Alliance™. OMA-TS-DM_StdObj-V1_2. URL:http://www.openmobilealliance.org
[DMTND]	“OMA Device Management Tree and Description, Version 1.2”. Open Mobile Alliance™. OMA-TS-DM_TND-V1_2. URL:http://www.openmobilealliance.org
[DMTNDS]	“OMA Device Management Tree and Description Serialization, Version 1.2”. Open Mobile Alliance™. OMA-TS-DM_TNDS-V1_2. URL:http://www.openmobilealliance.org
[EREIDCP]	“Enabler Release Definition for OMA Client Provisioning Specifications, version 1.1”. Open Mobile Alliance™. OMA-EREID-ClientProvisioning-V1_1. URL:http://www.openmobilealliance.org
[EREIDDM]	“Enabler Release Definition for OMA Device Management Specifications, version 1.2”. Open Mobile Alliance™. OMA-EREID-DM-V1_2. URL:http://www.openmobilealliance.org
[PKCS#15]	PKCS #15 v1.1: Cryptographic Token Information Syntax Standard”, RSA Laboratories, June 6, 2000. URL: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-15/pkcs-15v1_1.pdf
[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 Specification Version 1.1”. Open Mobile Alliance™. 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
[SCRRULES]	“SCR Rules and Procedures”, Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL:http://www.openmobilealliance.org/
[SCWS]	“Enabler Release Definition for Smartcard-Web-Server”, Open Mobile Alliance, OMA-EREID_Smartcard_Web_Server-V1_1, URL:http://www.openmobilealliance.org
[TS102.221]	“Smart Cards; UICC-Terminal interface; Physical and logical characteristics”, (ETSI TS 102 221 release 6), URL:http://www.etsi.org/
[TS151.011]	“Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface”, (ETSI TS 151 011), URL:http://www.etsi.org/
[WBXML1.1]	“WAP Binary XML Content Format Specification”, WAP Forum™. SPEC-WBXML-19990616.pdf. URL:http://www.openmobilealliance.org

- [WBXML1.2] “WAP Binary XML Content Format Specification”, WAP Forum™. WAP-154-WBXML.
[URL:http://www.openmobilealliance.org](http://www.openmobilealliance.org)
- [WBXML1.3] “WAP Binary XML Content Format Specification”, WAP Forum™. WAP-192-WBXML.
[URL:http://www.openmobilealliance.org](http://www.openmobilealliance.org)

2.2 Informative References

- [PushMO] “Push Management Object”. Open Mobile Alliance™, OMA-TS-Push_MO-V1_1.
[URL: http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [PushOTA] “Push Over The Air”, Open Mobile Alliance™, OMA_TS-PushOTA-V2_3,
[URL:http://www.openmobilealliance.org](http://www.openmobilealliance.org)
- [RFC2782] “A DNS RR for specifying the location of services (DNS SRV)”, A. Gulbrandsen et al., February 2000
[URL:http://www.ietf.org/rfc/rfc2782.txt](http://www.ietf.org/rfc/rfc2782.txt)
- [RFC4702] “The Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option”, M. Stapp et al., October 2006
[URL:http://www.ietf.org/rfc/rfc4702.txt](http://www.ietf.org/rfc/rfc4702.txt)
- [RFC4704] “The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option”, B. Volz, October 2006
[URL:http://www.ietf.org/rfc/rfc4704.txt](http://www.ietf.org/rfc/rfc4704.txt)
- [RFC5986] “Discovering the Local Location Information Server (LIS)”, M. Thomson et al., September 2010
[URL:http://www.ietf.org/rfc/rfc5986.txt](http://www.ietf.org/rfc/rfc5986.txt)

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

Kindly consult [DMDICT] for all definitions used in this document.

3.3 Abbreviations

Kindly consult [DMDICT] for all abbreviations used in this document.

4. Introduction

Other OMA DM specifications define how a management session is established and maintained. However, in order for a DM Client to be able to initiate a management session, it must be provisioned with OMA DM settings.

Bootstrap is the process of provisioning the DM Client to a state where it is able to initiate a management session to a new DM Server. DM Clients that have already been bootstrapped can be further bootstrapped to enable the DM Client to initiate a Management Session to new DM Servers or may be rebootstrapped to update existing accounts.

5. Bootstrapping

5.1 Bootstrap scenarios

OMA DM Clients need to be able to operate in different network environments and using a large set of protocols. This makes it hard to find a 'one size fits all' solution to the bootstrap problem. This section starts with the most basic requirements for bootstrap and continues to define three different processes for bootstrap

5.1.1 Requirements

An OMA DM solution capable of transforming an empty, clean DM Client into a state where it is able to initiate a management session needs to address these requirements.

- Re-use technology (WAP Push, HTTP Push)
- Tightly standardized and simple \Rightarrow Highly interoperable
- Self sufficient and complete
- Secure (signed and authenticated)
- Data format should be XML based
- Content mappable to OMA DM management objects
- Transport encoding should be [WBXML1.1], or [WBXML1.2], or [WBXML1.3]

5.1.2 Solutions

This document defines the following ways to perform the bootstrap process.

- Customized bootstrap
Devices are loaded with OMA DM account and connectivity information at manufacture. Also referred to as factory bootstrap.
- Bootstrap from smartcard
The smartcard is inserted in the Device and the DM Client is bootstrapped from the smartcard.
- Server initiated bootstrap
DM Server sends out Bootstrap Message via some push mechanism, e.g. WAP Push or OBEX. DM Server needs to receive the Device address/phone number beforehand.
- Client initiated bootstrap
DM Client retrieves the Bootstrap Message from a DM Bootstrap Server, whose URL is known to the Device a priori.

The DM Client **MUST** support at least one of these processes for each of the supported profiles (see section 5.3).

5.1.2.1 Customized bootstrap

This is a convenient way to bootstrap a DM Client from an end user perspective because the user does not have to do anything. In this scenario, an operator orders the Devices pre-configured from a device manufacturer. All the information about the operator's network and device management infrastructure is already in the Devices when they leave the factory. Another advantage of this method is that it is very secure. There is no need to transport sensitive commands and information, e.g. shared secrets, over the air. The method is however not very flexible and not all device manufacturers may provide this service. Not all Devices are sourced via the operator. In this scenario, either the DM Server or the DM Client initiates an OMA DM Management Session after user personalizes and bootstraps the DM Client.

Figure 1 gives an overview of this scenario.

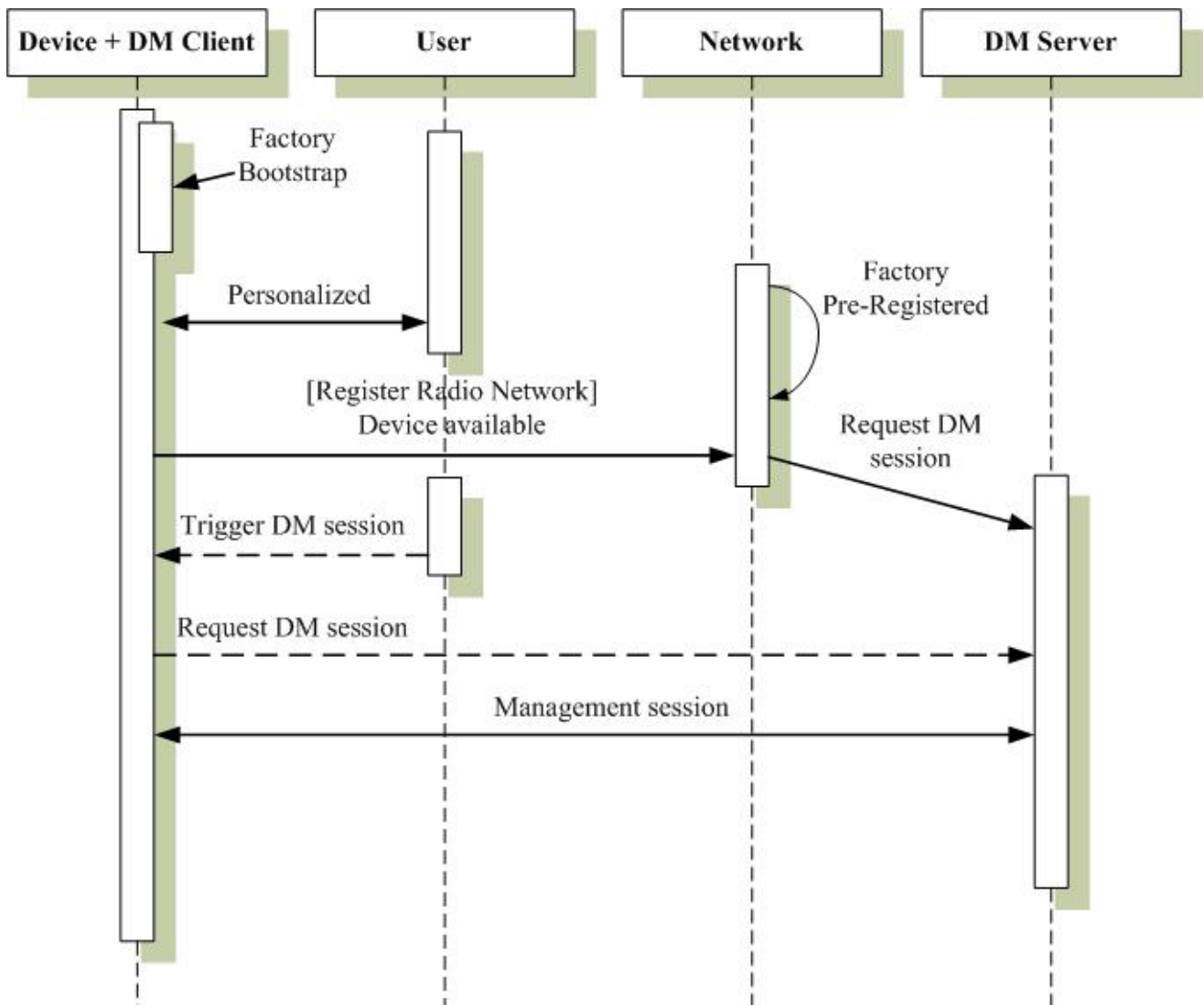


Figure 1: Customized bootstrap

5.1.2.2 Bootstrap from smartcard

This is a convenient way to bootstrap a DM Client from an end user perspective because the user does not have to do anything. In this scenario the DM Client is able to obtain the Bootstrap Message from the smartcard. There is no need to transport sensitive bootstrap commands and information, e.g. shared secrets, over the air. The smartcard is secure, ensuring that the Bootstrap Message is authorized. A Device supporting the smartcard can be bootstrapped for DM without necessarily being purchased from the operator. In this scenario, either the DM Server or the DM Client initiates a Management Session after DM Client bootstraps.

Figure 2 gives an overview of this scenario.

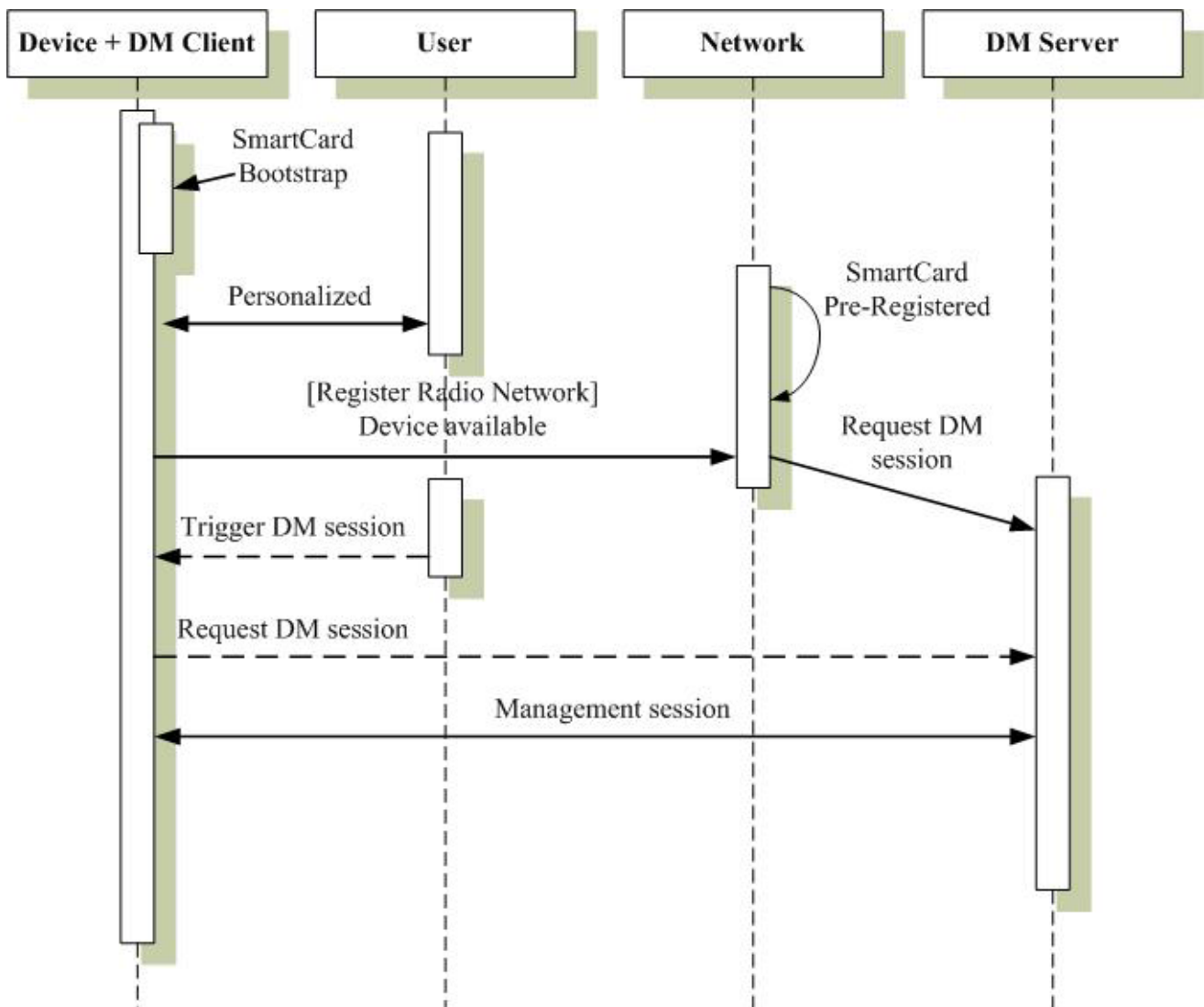


Figure 2: Bootstrap from smartcard

5.1.2.3 Server initiated bootstrap

In this scenario, the Devices leave the assembly line in a clean and empty state. Once a user acquires a Device and personalizes it, e.g. by inserting a SIM, the prerequisites for this process are in place. The problem is now to inform the DM Server of the identity, address or phone number of the device and this can be achieved in many ways.

- It could be done at the point-of-sales where a sales system ties in with the management system and delivers the information.
- It could be done through a self-service web site where the user enters her own phone number.
- It could be done by the network the first time the Device registers to the network. When this happens a trigger could be sent from the core network to the DM Server with the number used by the Device.
- It could be done with a voice prompt system where the user is prompted to key in her phone number.

Regardless of how the phone number or Device address reaches the DM Server, the DM Server is now in a position where it can send out a Bootstrap Message. This message, whose structure and content are defined in this document, contains enough

information for the DM Client to be able to initiate a management session with the device management server that sent out the Bootstrap Message.

The DM Clients SHOULD accept Bootstrap Messages only from authorized servers [DMSecurity].

Figure 3 gives an overview of this scenario.

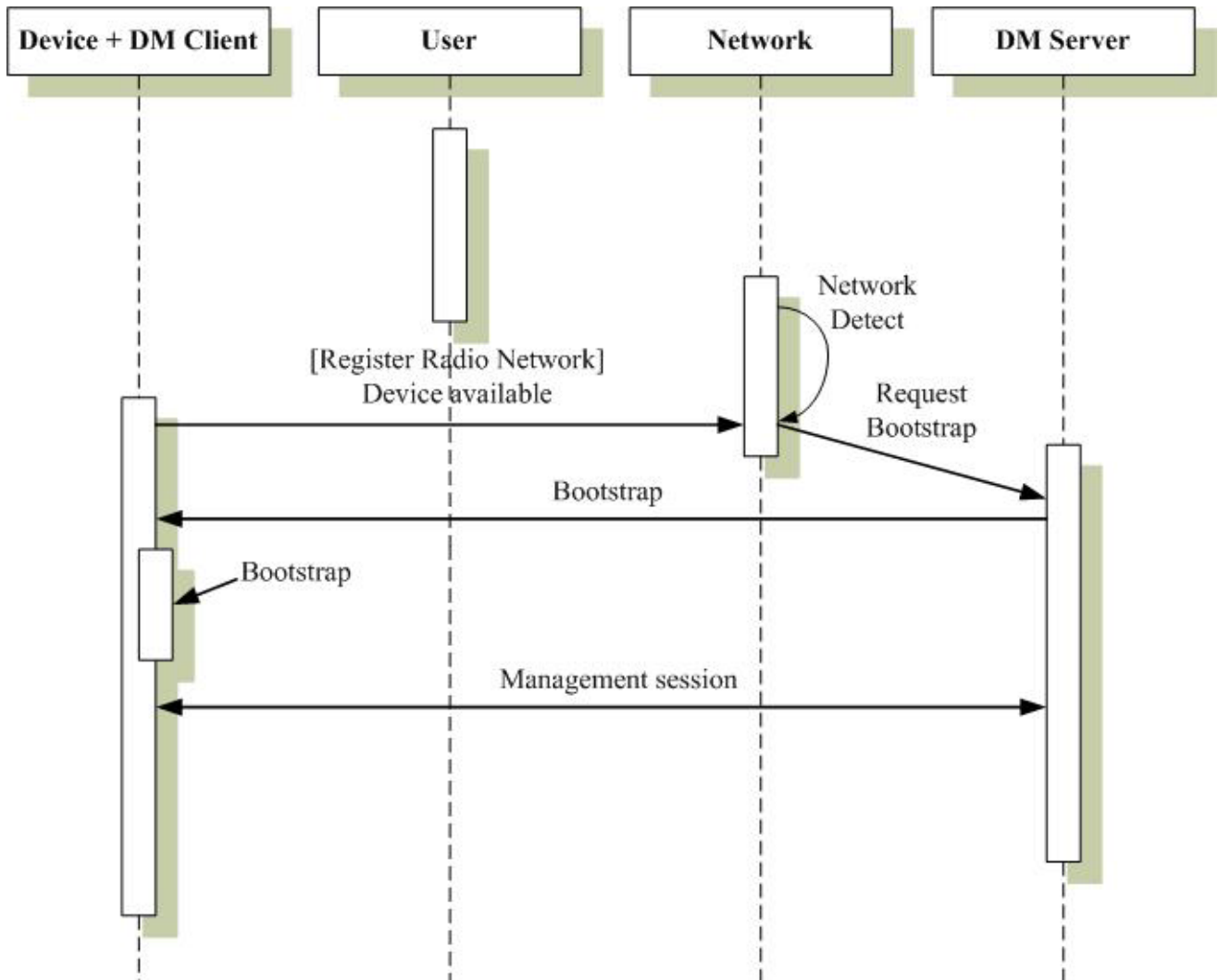


Figure 3: Server initiated bootstrap

5.1.2.4 Client initiated bootstrap

In this scenario, the DM Client retrieves the bootstrap package from a DM Bootstrap Server, whose URL is known to the Device a priori, as shown in Figure 4; in Appendix E a method to discovery Bootstrap Server is described. After the bootstrap package gets installed successfully, the DM Client attempts to initiate a management session with the DM Server.

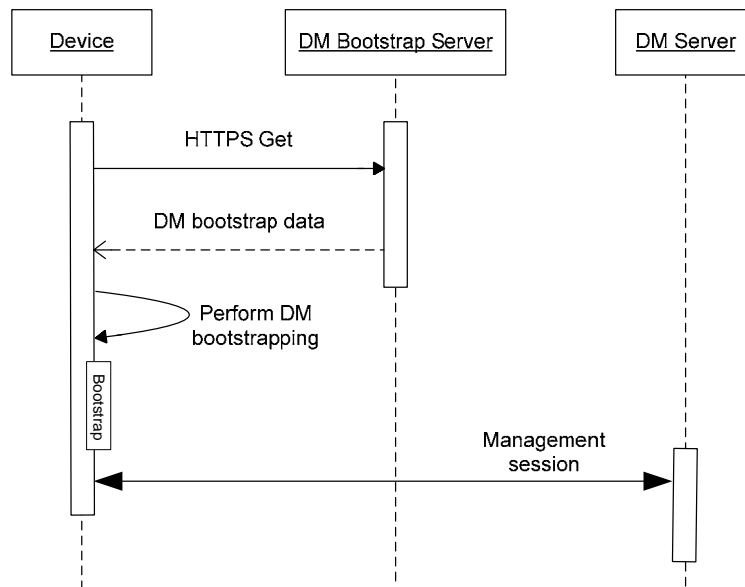


Figure 4: Client initiated bootstrap

5.2 OTA Bootstrap Package Delivery (Informative)

OTA (Over-the-air) delivery of the DM bootstrap package is based on OMA Push [PushOTA][PushOTA][PushOTA][PushOTA][PushOTA]. The policy that the Device consults to decide if a bootstrap package will be accepted is outside the scope of this specification. One approach is for a Device to support the Push Management Object [PushMO], which maintains a “White List” of entities that are authorized to send OMA Push messages to the Device. In this case the Device will process the Push message only if it originates from an authorized entity.

5.3 Bootstrap profiles

OMA DM has been designed to meet the management requirements of many different types of devices. For some of these device types there already exists a bootstrap or provisioning mechanism. In these cases OMA DM leverages the existing mechanisms so that backwards compatibility and simple deployment can be achieved. To define how different kinds of devices can be bootstrapped and to specify how OMA DM leverages existing standards this document introduces the concept of bootstrap profiles. Each profile defines its own security, transport and data format.

Currently two profiles are planned, but as interest in OMA DM grows and usage of it increases more profiles can be added.

The Device Management Profile **MUST** be supported. Any other particular profile **MAY** be supported.

OMA Client Provisioning

This profile specifies alignment of two existing enablers – OMA Client Provisioning [ERELDCP] and OMA Device Management [ERELDDM]. This profile defines how the information provisioned using OMA Client Provisioning can be transferred to the management tree specified in the OMA Device Management. In this profile at least the mapping of w7 (DM account) information to the management tree needs to be supported, but other provisioning information can also be mapped to the management tree.

OMA Device Management

This profile defines how the OMA Device Management [ERELDDM] can be used for bootstrapping.

5.4 OMA Client Provisioning Profile

OMA Client Provisioning enabler [ERELDCP] is designed to provision the initial configuration information to Devices, and can be used to enable a device to be managed by OMA Device Management enabler [ERELDDM]. The chapter specifies the mapping of the Client Provisioning information to the Device's management tree in a way that later management for the provisioned parameters is possible in case both Client Provisioning and Device Management enablers are supported by the Device.

The content of the provisioning message is based on the OMA Provisioning Content Specification [PROVCONT]. In order to enable the usage of the OMA Provisioning Content Specification within the OMA Device Management framework, the DM application registration document w7 [ACw7DM] is released by DM group to provide information how the APPLICATION characteristic in OMA Provisioning content [PROVCONT] is used to provision OMA Device Management enabler [ERELDDM] parameters.

5.4.1 Transports

Bootstrapping using OMA Client Provisioning profile is done as defined in the OMA Client Provisioning Bootstrap specification [PROVBOOT].

5.4.2 Mapping Characteristic Data to the Management Tree

When Device receives Client Provisioning document, the DM Client creates a management object for each application characteristic in the DM management tree. Management object can have two different types of name space identifiers (Property Name described in [DMTND]) - One where the name is already given in the DDF [DMTND] and another where the name is dynamic separating the instances of the child nodes (see Figure 5).

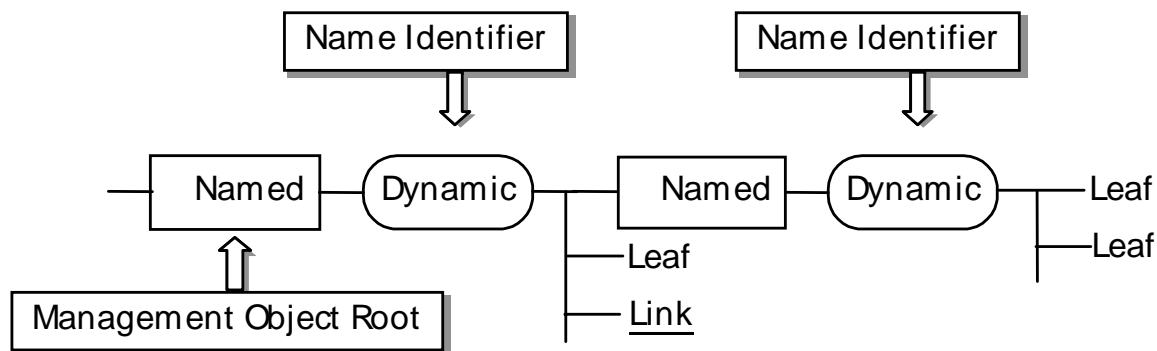


Figure 5: Example Management Object and Name Identifiers

The name identifiers for named nodes are already given in the management object DDF. Also, the parameter mapping between Client Provisioning parameters and Management Object parameters MAY be specified in the Management Object specification. In addition a general rule that SHOULD be followed to map named information between Client Provisioning APPLICATION characteristic and standardized Connectivity Management Object template structure is given in Appendix C.

The DM Client gives the name identifiers for dynamic nodes that are separating the instances of the child nodes. Though the format of name identifiers for these dynamic nodes is implementation specific, a client MAY assign numeric identifiers starting from '1' and increasing by one every time. In this case and when there is priority specified in the Provisioning Content document the rank SHOULD reflect that.

5.4.3 Management Object Location in the Management Tree

Newly created management object location in the management tree is decided by the DM Client. However, it **MUST** be placed following the published DDF of the management tree so that the server is able to know where to find the provisioned information.

5.4.4 Management Object Access Rights

All provisioning information mapped from the Provisioning Content [PROVCONT] document to management tree **MUST** be granted Get, Replace and Delete ACL rights to the ServerID specified in the w7 APPLICATION characteristic provisioned inside Provisioning Content message. The management authority owning the ServerID may modify this ACL in a subsequent DM session.

In case w7 APPLICATION characteristic is not part of the provisioning message the Device receiving the message and mapping the information to the DM management tree **MUST NOT** give the access rights to these parameters to the improper management authority.

5.4.5 Special Behaviors - Smart Card Provisioning

In case Smart Card contains the provisioning information as specified in the [PROVSC], the Device **SHOULD** detect the removal and/or change of the Smart Card. When the Smart Card is removed and/or changed, the DM Client **SHOULD** remove all the provisioned management object information (originated from the Smartcard) from the DM management tree.

5.4.6 Device Management, Access Point and Proxy Information

Devices supporting both Client Provisioning and Device Management **MUST** be able to map w7 (Device Management account) and NAPDEF (if supported) and PROXY (if supported) characteristics information to the DM management tree. The mapping of the named nodes is specified in [DMSTDOBJ]. An explicit mapping of w7 to DMAcc is provided in Appendix C of [DMSTDOBJ], a general mapping of application characteristics can be found in Appendix C of this document.

The DM Client **MUST** give the names for the dynamic nodes as described in Section 5.4.2.

5.4.7 Other Client Provisioning information

Devices supporting both Client Provisioning and Device Management **MAY** decide to map other information provisioned in the Client Provisioning message to the DM management tree. In case a specific mechanism is described in the Management Object document that mapping **MUST** be followed.

5.5 OMA Device Management Profile

The OMA DM Bootstrap Profile includes procedures by which a DM Client installs or updates the DMAcc [DMSTDOBJ] MO, upon receiving a TNDS [DMTNS] encoded Bootstrap Message. Additionally other MOs may also be installed or updated.

The content of the Bootstrap Message is a standard OMA DM message. DM Clients **MUST** support embedded WBXML encoded TNDS objects and normal TNDS objects and **MUST** support the Inbox. In order to be bootstrapped successfully, the DM client requires both DM account information and connectivity information. It is **RECOMMENDED** to use standardized connectivity MOs to represent the connectivity information.

5.5.1 Transport

See the security document for transport and security information [DMSecurity].

5.5.2 Management tree ACL and bootstrap

The policy that the Device consults to decide if a Bootstrap Message will be accepted is outside the scope of this specification. If a Bootstrap Message is accepted it MUST be processed according to the conditions described in section 5.5.5.

5.5.3 Management Object Access Rights

When a Bootstrap Message adds new TNDS objects, any ACL values that are to be set for these objects MUST be included in the TNDS data as ACL property data for the applicable nodes.

5.5.4 Bootstrap Message Content

The content of a Bootstrap Message is a normal DM Message. However, it is a special package in many ways since it is not part of an ongoing OMA DM session but rather a one-time message. Hence, many of the elements needed to manage the session are superfluous in this context, but they must still be included so that the message may be processed by the normal DM Client.

A Bootstrap Message MUST set the values for the DMAcc management object defined in [DMSTDOBJ]. Other values (such as connectivity settings) MAY also be set.

The value of the SyncHDR/Source/LocURI element for a Bootstrap Message MUST match the value of one of the AppAddr/<x>/Addr nodes of a DMAcc object in that Bootstrap Message.

DM Bootstrap Message MUST be [WBXML1.1], or [WBXML1.2], or [WBXML1.3] encoded.

DM Servers MUST NOT expect any response message for a Bootstrap Message. An implicit acknowledgement of successful processing of a Bootstrap Message can be concluded when the client connects to the server for the first Management Session.

See the DM Security document [DMSecurity] for information on security and encryption.

5.5.5 Processing of the Bootstrap

A Bootstrap Message is processed just like a normal DM Message, except that a response message MUST NOT be sent back.

The DM Client MAY rename a new MO. In the case of the Connectivity MO the DM Client SHOULD also rename the values of the corresponding connectivity references to the new name for all MO's encoded within the same TNDS object.

When a TNDS object contains a MO where connectivity references are linked to a Connectivity or Proxy MO that also are included in the same TNDS object, then the values of those connectivity references MAY contain a URI that starts with “./Inbox”. In that case the URI MUST have the value of “./Inbox/” plus the URI of that Connectivity MO's location in the same TNDS object.

This is an example of a TNDS object where only part of the TNDS object is shown:

```
<MgmtTree>
  <VerDTD>1.2</VerDTD>
  <Node>
    <NodeName>OperatorX</NodeName>      <!-- DM Account MO -->
    <RTProperties>
      <Format>
        <node/>
      </Format>
      <Type><DDFName>org.openmobilealliance/1.0/w7</DDFName></Type>
    </RTProperties>
```

```

<Node>
  <NodeName>PrefConRef</NodeName>
  <RTProperties>
    <Format>
      <chr/>
    </Format>
    <Type><MIME>text/plain</MIME></Type>
  </RTProperties>
  <Value>./Inbox/Internet</Value>
</Node>
...
<NodeName>Internet</NodeName>      <!-- Connectivity MO -->
<RTProperties>
  <Format>
    <node/>
  </Format>
  <Type><DDFName>org.openmobilealliance/1.0/ConnMO</DDFName></Type>
</RTProperties>
...
</Node>
</MgmtTree>

```

If a DM Client encounters an item with an URI of the EXT sub-tree that it is not prepared to handle, the DM Client MAY ignore that item so that the message may succeed.

After successfully processing the Bootstrap Message, the DM Client SHOULD automatically initiate a Management Session to any DM Server configured in the Bootstrap Message at the next practical opportunity, subject to restrictions and configuration in the DMAcc of each bootstrapped server (i.e., when network connectivity and other factors would allow such a connection).

If the Bootstrap Message contains a MO that the DM Client does not support, the DM Client MAY ignore this MO, so that the message may succeed.

If the Bootstrap Message contains multiple versions of a MO, the DM Client SHOULD use the latest version of that MO that it supports and ignore the other versions, so that the message may succeed.

5.5.6 Smartcard

If the Device supports a smartcard, the DM Client MUST support detection, retrieval, and processing of Bootstrap Message from the smartcard as described in Appendix D. The DM Client MAY include configurable security policy to disable smartcard bootstrap functions. If the smartcard bootstrap function is enabled (i.e. no security policy is implemented or security policy does not disable smartcard bootstrap) and the smartcard has not been rejected by the device (for example, because of a SIM-locking mechanism), the DM Client SHALL retrieve the Bootstrap Message from the smartcard when the device is switched on and apply it to the device configuration.

The DM Client SHOULD check that the bootstrap data for all DM Servers previously bootstrapped from the smartcard are still available from the smartcard when the device is switched on; if not, the information for any DM Servers that were previously bootstrapped from the smartcard but are no longer stored on the smartcard SHOULD be removed from the Device Management tree.

5.5.7 Bootstrap via HTTPS Get

If the Device supports the HTTPS protocol, it MAY retrieve a Bootstrap Message from a URL by following these steps:

1. The device performs a HTTPS Get to a Bootstrap Server.
2. The Bootstrap returns the Bootstrap Message to the Device or indicates the Bootstrap Message is not available (e.g. returns error code 404).
3. If the Bootstrap Message is returned to the device, it is handed off to the DM Client.
4. Upon successful verification of the Bootstrap Message, the DM Client processes the Bootstrap Message as normal.

If the Device supports HTTPS protocol and [SCWS], it MAY retrieve a bootstrap message by following the above steps and using the following absolute URL: “https://{SCWS@}/OMA/DM/Bootstrap.xml”, where {SCWS@} depends on the transport and IP version supported as shown in the following table:

Transport	IP version	{SCWS@}
BIP (Note 1)	IPv4	127.0.0.1:4116
	IPv6	:::1:4116
TCP/IP	IPv4	localhost:443
	IPv6	localhost:443

(Note 1) The Device MAY use “localhost” host name instead of loopback address “127.0.0.1” for IPv4 or “[::1]” for IPv6.

6. Bootstrap Config MO

6.1 Introduction

The Bootstrap Config MO provides the ability to manage the bootstrap functionality on a Device. This MO MUST NOT be used to manage the initial access rights of the DM Server unless the DM Client is bootstrapped to at least one other DM Server.

Support for this MO is OPTIONAL.

6.2 Graphical Representation

(Informative)

Figure 6 gives the graphical representation of the Bootstrap Config MO.

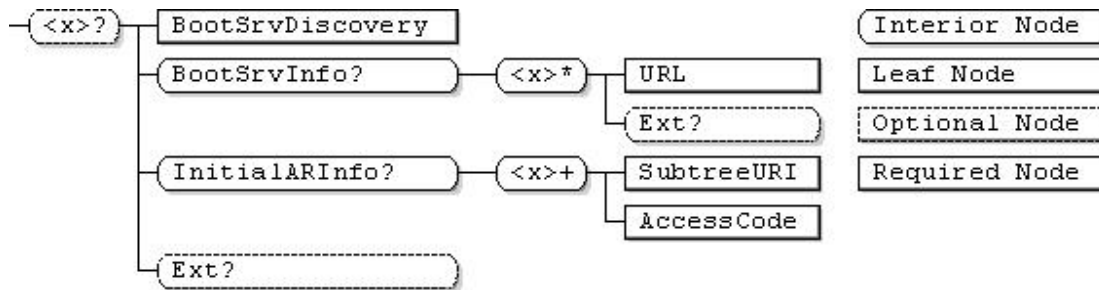


Figure 6: Bootstrap Config MO

6.3 Node Descriptions

This section provides the description of the various nodes within the Bootstrap Config MO.

.../<x>

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This placeholder node is the root node for the Bootstrap Config MO. The parent node of this node defines the location of this MO in the Management Tree.

The Management Object Identifier for the Bootstrap Config MO MUST be: “urn:oma:mo:oma-dm-bootstrapcfg:1.0”.

<x>/BootSrvDiscovery

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get, Replace

This leaf node indicates whether or not the Device is allowed to discover a DM Bootstrap Server. The permitted values for this node are shown in the following table.

0	The Device is inhibited from discovering the DM Bootstrap Server.
1	The Device is allowed to discover the DM Bootstrap Server.

The default value for this node is left to implementations.

<x>/BootSrvInfo

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node is the parent node of the subtree that stores the DM Bootstrap Server URLs, along with the pertinent credential and access rights information.

<x>/BootSrvInfo/<x>

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This placeholder node is the root node for all the information pertaining to one DM Bootstrap Server.

<x>/BootSrvInfo/<x>/URL

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get, Replace

The value of this leaf node is the URL of a DM Bootstrap Server.

<x>/BootSrvInfo/<x>/Ext

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node is for vendor specific extensions for managing DM Bootstrap Server URLs on the Device.

<x>/InitialARInfo

Status	Occurrence	Format	Min. Access Types
Required	ZeroOrOne	node	Get

This interior node is the root node for all the initial access rights information. If this node is not present, the initial ACL access rights are assumed to be as per the device policy.

<x>/InitialARInfo/<x>

Status	Occurrence	Format	Min. Access Types
Required	OneOrMore	node	Get, Add, Delete

This placeholder node is the root node for the initial access rights information for one subtree within the Management Tree.

<x>/InitialARInfo/<x>/SubtreeURI

Status	Occurrence	Format	Min. Access Types
Required	One	chr	Get, Replace

This value of this leaf node is the URI of the root of a subtree within the Management Tree.

<x>/InitialARInfo/<x>/AccessCode

Status	Occurrence	Format	Min. Access Types
Required	One	int	Get, Replace

This node specifies initial access rights that the DM Server is granted on the subtree, whose root is specified by the value of SubtreeURI node, upon successful completion of the Bootstrap procedure. The valid value of this node is any Access Type value from the following table, or any value obtained from the bit-wise ORing of the Access Type values:

Access Type	Value
Get	1 (i.e. 0x1)
Replace	2 (i.e. 0x2)
Exec	4 (i.e. 0x4)
Copy	8 (i.e. 0x8)
Add	16 (i.e. 0x10)
Delete	32 (i.e. 0x20)

For example, if the ACL rights are only Get, the value of this node is 1. If the ACL rights are Get, Add and Delete, the value of this node is 49.

If the value of the SubtreeURI node does not correspond to a node in the Management Tree then the value of this node MUST be ignored.

<x>/Ext

Status	Occurrence	Format	Min. Access Types
Optional	ZeroOrOne	node	Get

This interior node is for vendor specific extensions for managing the client initiated bootstrap functionality on a Device.

Appendix A.

(Informative)

A.1 Approved Version History

Reference	Date	Description
N/A	N/A	No prior 1.3 version.

A.2 Draft/Candidate Version 1.3 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-TS-DM_Bootstrap-V1_3	15 Oct 2008	All	Baseline to v1.3 using OMA-TS-DM_Bootstrap-V1_2.
	21 May 2009	2.1, 5.4	Applied OMA-DM-DM13-2009-0023-CR_Bootstrap_Security.
	01 Jun 2009	5.4.7	Applied OMA-DM-DM13-CR_URL_Bootstrap OMA-DM-2008-0158R01-CR_Mandatory_Bootstrap.
	06 Jul 2009	2.1, 5.4.4	Applied OMA-DM-DM13-2009-0030-CR_Remove_Bootstrap_XML_Security.
	08 Sep 2009	All	Applied OMA-DM-DM13-2009-0064R02-CR_SC_bootstrap_patch.
	17 Nov 2009	All	Applied OMA-DM-DM13-2009-0077R03-CR_Bootstrap_Cleanup OMA-DM-DM13-2009-0084R02-CR_Bootstrap_is_Mandatory
	10 Dec 2009	5.4, B	Applied OMA-DM-DM13-2009-0116R02-CR_Bootstrap_WBXML
	29 Dec 2009	All	Corrected grammar, spelling and other clerical errors.
	11 Jan 2009	All	More spelling errors corrected, applied OMA-DM-DM13-2009-0132-CR_Bootstrap_Figure_Clarification.
	04 Feb 2010	All	Applied OMA-DM-DM13-2010-0008R01-CR_Bootstrap_bugfix OMA-DM-DM13-2010-0029R01-CR_Boot_missing_SCR OMA-DM-DM13-2010-0031R01-CR_Boot_clarification OMA-DM-DM13-2010-0028R01-CR_Bootstrap_Fixes_Again.
	10 Feb 2010	All	General editorial clean-up by DSO.
	23 Mar 2010	5.4.7	Changed blue text to black.
	14 Apr 2010	5.1.1	Editorial change to remove "SIP Push".
	26 Apr 2010	All	Creation by DSO of a clean version without change marks.
05 May 2010	5.4.5, 5.4.7	Formatting of an example Formatting of a note.	
Candidate Version OMA-TS-DM_Bootstrap-V1_3	25 May 2010	N/A	Status changed to Candidate by TP Ref # OMA-TP-2010-0221- INP_DM_V1.3_ERP_and_ETR_for_Candidate_approval
Draft Versions OMA-TS-DM_Bootstrap-V1_3	25 Aug 2010	5.4.1, 5.4.4, 5.4.7	Applied OMA-DM-DM13-2010-0087-CR_Bootstrap_Security OMA-DM-DM13-2010-0067R02- CR_Bootstrap_via_HTTPS_Get_Cleanup
	20 Sep 2010	5.4.4	Applied OMA-DM-DM13-2010-0106R01- CR_Bootstrap_LocURI_value_clarification
Candidate Version OMA-TS-DM_Bootstrap-V1_3	07 Dec 2010	N/A	Status changed to Candidate by TP Ref # OMA-TP-2010-0502- INP_DM_V1_3_ERP_and_ETR_for_Candidate_re_approval
Draft Versions OMA-TS-DM_Bootstrap-V1_3	19 Apr 2011	All	Applied OMA-DM-DM13-2011-0022R04-CR_DMBBoot_Restructuring OMA-DM-DM13-2011-0027R05-CR_Bootstrap_Config_MO OMA-DM-DM13-2011-0029R03- CR_Client_Initiated_Bootstrap_and_DM_Bootstrap_Discovery

Document Identifier	Date	Sections	Description
	18 Jul 2011	2.2, 3.3, 5.2	Applied OMA-DM-DM13-2011-0055R01-CR_OTA_Bootstrap_Pkg_Delivery
	02 Sep 2011	5.1.2.5	Applied OMA-DM-DM13-2011-0083-CR_Bootstrap_Server_Update
Draft Versions OMA-TS-DM_Bootstrap-V1_3	14 Oct 2011	All	Applied OMA-DM-DM13-2011-0073R02-CR_Initial_Access_Rights OMA-DM-DM13-2011-0091-CR_Bootstrap_Editorial Informative references sorted in alphabetical order
	05 Jan 2012	All	Applied OMA-DM-DM13-2011-0127R03-CR_CONR_Bootstrap
	06 Jan 2012	6.2	Applied OMA-DM-DM13-2011-0151-CR_CONR_Bootstrap_part_2
	20 Jan 2012	All	Applied OMA-DM-DM13-2012-0007-CR_AP_Bootstrap_Fix Applied 2012 TS template according to AI DM-2012-A006 + added reference to SCRRULES and deleted reference to IOPPROC accordingly Restored cross-references to sections in SCR tables Applied 2012 template to introduction section.
	26 Jan 2012	All	Created cross-references in the whole document according to Action Item DM-2012-007 Version in PushOTA reference changed to 2.3 according to Action Item DM-2012-007
	31 Jan 2012	All	Applied OMA-DM-DM13-2012-0027-CR_removing_reference_ISO7816_4 OMA-DM-DM13-2012-0028-CR_Bootstrap_Editorials Restored two cross-references in one SCR table.
	09 Feb 2012	5.1.2.3, App B 3, App E	Applied OMA-DM-DM13-2012-0022-CR_TS_Boot_SCR OMA-DM-DM13-2012-0024-CR_CONR_resolution_Bootstrap
	22 Feb 2012	6.3	Applied OMA-DM-DM13-2012-0078R02-CR_BootstrapTS_Reformat_BootstrapConfigMO
	23 Feb 2012	4.1	Header removed by DSO according to Action Item DM-2012-A030
Candidate Version OMA-TS-DM_Bootstrap-V1_3	06 Mar 2012	N/A	Status changed to Candidate by TP Ref # OMA-TP-2012-0084-INP_DM_V1_3_ERP_and_ETR_for_Candidate_re_approval
Draft Version OMA-TS-DM_Bootstrap-V1_3	16 Aug 2012	6.3	Incorporated CR: OMA-DM-DM13-2012-0106-CR_BootstrapConfigMO_Editorial
Candidate Version OMA-TS-DM_Bootstrap-V1_3	09 Oct 2012	n/a	Status changed to Candidate by TP TP Ref # OMA-TP-2012-0368R01-INP_DM_V1_3_ERP_and_ETR_for_Candidate_re_approval

Appendix B. Static Conformance Requirements (Normative)

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

B.1 SCR for Bootstrap Client

Item	Function	Reference	Requirement
DM-BOOT-C-001-M	Support for at least one bootstrap mechanism	Section 5.1.2	
DM-BOOT-C-002-O	Support for OMA Client Provisioning Profile	Section 5.3	ProvBoot:ProvBoot-B-C-001 AND DM-BOOT-C-004
DM-BOOT-C-003-M	Support for OMA Device Management Profile	Section 5.3	
DM-BOOT-C-004-O	Provisioning Content granted Get, Replace and Delete ACL rights to ServerID in w7	Section 5.4.4	
DM-BOOT-C-005-O	Support for OMA Client Provisioning Profile AND OMA Device Management	Section 5.4.6	DM-BOOT-C-006-O
DM-BOOT-C-006-O	Map w7, NAPDEF (if supported) and PROXY (if supported) to management tree	Section 5.4.6	
DM-BOOT-C-007-O	Device supports a Smartcard	Section 5.5.6	DM-BOOT-C-008-O
DM-BOOT-C-008-O	DM Client is capable of detecting, retrieving, and processing DM Profile bootstrap data from the Smartcard	Section 5.5.6	
DM-BOOT-C-009-O	Smartcard bootstrap function is enabled by DM client and the smartcard has not been rejected by the device	Section 5.5.6	DM-BOOT-C-010-O AND DM-BOOT-C-013-O
DM-BOOT-C-010-O	Device retrieves bootstrap data from the Smartcard and applies it to the device configuration	Section 5.5.6	
DM-BOOT-C-011-M	Support for embedded WBXML encoded TNDIS objects and normal TNDIS objects	Section 5.5	
DM-BOOT-C-012-M	Support for Inbox	Section 5.5	
DM-BOOT-C-013-O	DM Client removes the DM Server's information from the Device Management Tree if they are no longer stored on the smartcard when the device is switched on	Section 5.5.6	
DM-BOOT-C-014-O	Device supports SCWS and	Section 5.5.7	DM-BOOT-C-015-O

Item	Function	Reference	Requirement
	HTTPS		
DM-BOOT-C-015-O	Device retrieves Bootstrap Message from Smartcard URL using HTTPS Get	Section 5.5.7	
DM-BOOT-C-016-M	Support for WBXML encoded DM Bootstrap Messages	Section 5.5	

B.2 SCR for Bootstrap Server

Item	Function	Reference	Requirement
DM-BOOT-S-001-O	Support for OMA Client Provisioning Profile	Section 5.3	
DM-BOOT-S-002-M	Support for OMA Device Management Profile	Section 5.3	
DM-BOOT-S-003-M	Encode DM Bootstrap Message into WBXML	Section 5.5	
DM-BOOT-S-004-M	Support for embedded WBXML encoded TNDIS objects and normal (non-WBXML-encoded) TNDIS objects.	Section 5.5	

B.3 SCR for Bootstrap Config MO

B.3.1 SCR for Bootstrap Config MO tree structure

Item	Function	Reference	Requirement
BOOTCFGMO-T-001-O	Use of appropriate Management Object identifier	Section 6.3	BOOTCFGMO-T-002-O AND BOOTCFGMO-T-004-O
BOOTCFGMO-T-002-O	Support for Required nodes under root node	Section 6.3	
BOOTCFGMO-T-003-O	Support for Optional nodes	Section 6.3	BOOTCFGMO-T-001-O
BOOTCFGMO-T-004-O	Support for Required nodes under an Optional node if the Optional node is supported	Section 6.3	

B.3.2 SCR for Bootstrap Config MO functionality

Item	Function	Reference	Requirement
BOOTCFGMO-C-001-M	Support to allow discovery of DM Bootstrap Server	Section 6.3	

Item	Function	Reference	Requirement
BOOTCFGMO-C-002-M	Support to inhibit discovery of DM Bootstrap Server	Section 6.3	
BOOTCFGMO-C-003-M	Support a smartcard to retrieve the Bootstrap Server URL from the smartcard.	Section 6.3	
BOOTCFGMO-S-001-M	Support for the Bootstrap Config Management Object	Section 6.3	

B.3.3 SCR for DM System

Item	Function	Reference	Requirement
BOOTCFGMO-001-M	Provide value for URL of a DM Bootstrap Server	Section 6.3	

Appendix C. General Mapping

In the below table the Provisioning Content APPLICATION characteristic correspondence is shown to the Structure Template for Application Connectivity Management Object.

APPLICATION CHARACTERISTIC INFORMATION	STRUCTURE TEMPLATE FOR APPLICATION CONNECTIVITY MANAGEMENT OBJECT
APPID	AppID
PROVIDER-ID	ProviderID
NAME	Name
AACCEPT	AAccept
APROTOCOL	AProtocol
TO-PROXY	PrefConDef, if multiple ToConRef / <X> / ConRef
TO-NAPID	PrefConDef, if multiple ToConRef / <X> / ConRef
ADDR	PrefAddr
APPADDR / ADDR	AppAddr / <X> / Addr
APPADDR / ADDRTYPE	AppAddr / <X> / AddrType
APPADDR / PORT / PORTNBR	AppAddr / <X> / Port / <X> / PortNbr
APPADDR / PORT / SERVICE	AppAddr / <X> / Port / <X> / Service / <X> / Service
APPAUTH / AAUTHLEVEL	AppAuth / <X> / AAuthLevel
APPAUTH / AAUTHTYPE	AppAuth / <X> / AAuthType
APPAUTH / AAUTHNAME	AppAuth / <X> / AAuthName
APPAUTH / AAUTHSECRET	AppAuth / <X> / AAuthSecret
APPAUTH / AAUTHDATA	AppAuth / <X> / AAuthData
RESOURCE / URI	Resource / <X> / URI
RESOURCE / NAME	Resource / <X> / Name
RESOURCE / AACCEPT	Resource / <X> / AAccept
RESOURCE / AAUTHTYPE	Resource / <X> / AAuthType
RESOURCE / AAUTHNAME	Resource / <X> / AAuthName
RESOURCE / AAUTHSECRET	Resource / <X> / AAuthSecret
RESOURCE / AAUTHDATA	Resource / <X> / AAuthData
RESOURCE / STARTPAGE	N/A

Table 1: General Mapping

Appendix D. Storage of DM Bootstrap Message on the Smartcard (Normative)

We can sort out three main types of smartcards used for wireless telecom networks, characterised by their physical and logical characteristics:

- SIM smartcards platforms [TS151.011]
- UICC smartcards platforms [TS102.221]
- R-UIM smartcards platform [C.S0023-B_v1.0]

This section aims at specifying the storage mechanism of Bootstrap Message on such smartcard platform type.

For the purposes of this document the R-UIM is to be treated according to the rules defined for the SIM.

D.1 File structure

The information format is based on [PKCS#15] specification. The Bootstrap Message is located under the PKCS#15 directory allowing the card issuer to decide the identifiers and the file locations. The smartcard operations that are relevant include:

- Application selection
- Cardholder verification
- File access (select file, read, write)

The [PKCS#15] specification defines a set of files. Within the PKCS#15 application, the starting point to access these files is the Object Directory File (ODF). The EF(ODF) contains pointers to other directory files. These directory files contain information on different types of objects (authentication objects (PIN), data objects, etc). For the purpose of Bootstrap Message, EF (ODF) MUST contain the EF Record describing the DODF-bootstrap. The EF(ODF) is described in section D.4.1 and [PKCS#15].

EF(ODF) contains pointers to one or more Data Object Directory Files (DODF) in priority order (i.e. the first DODF has the highest priority). Each DODF is regarded as the directory of data objects known to the PKCS#15 application. For the purposes of DM bootstrapping, EF(DODF-bootstrap) contains pointer to the Bootstrap Message, namely DM_Bootstrap File. The EF(DODF-bootstrap) is described in section D.4.2 and [PKCS#15].

The provisioning files are stored as PKCS#15 opaque data objects.

The support of smartcard Bootstrap Message will be indicated to the ME's user agent, by the presence in the EF DIR (see [TS102.221]) of an application template as defined here after.

The RECOMMENDED format of EF(DIR) is a linear fixed record in order to be in line with [TS102.221].

EF (DIR) MUST contain the application template used for a PKCS#15 application as defined in [PKCS#15]. Application template MUST consist of Application identifier (tag 0x4F) and Path (tag 0x51) information.

The EF(ODF) and EF(DODF-bootstrap) MUST be used by the ME to determine the path of the DM_Bootstrap file.

UICC smartcard platforms can support two modes of activation: 2G and 3G. UICC smartcard platform activated in a 2G mode has the logical characteristics of the SIM smartcard platform [TS151.011]. In that case, smartcard operations for accessing the Bootstrap Message conform to the ones defined for the SIM as specified in section D.2.

UICC smartcard platform activated in a 3G mode has the physical and logical characteristics according to [TS102.221]. In that case, smartcard operations for accessing the Bootstrap Message are specified in section D.3.

D.2 Bootstrap Message on SIM or UICC activated in 2G mode

D.2.1 Access to the file structure

To select the PKCS15 application, the Device MUST evaluate the PKCS#15 application template present in the EF (DIR), then the Device MUST use the indirect selection method as defined in [TS151.011] to select the application.

D.2.2 Files Overview

The file structure for the Bootstrap Message within the SIM smartcard is described below.

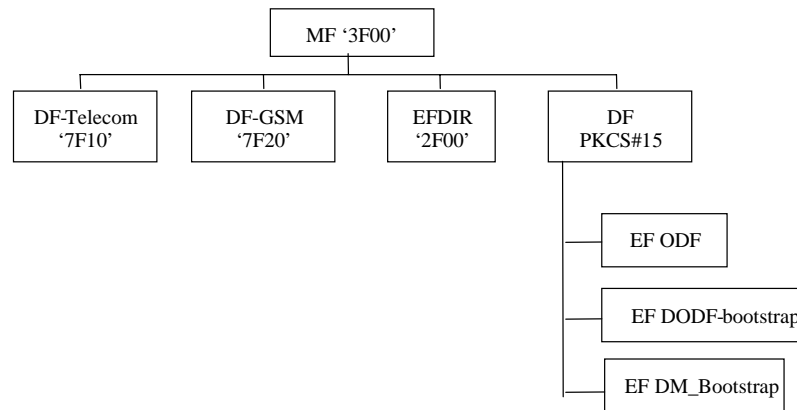


Figure 7: File structure for Bootstrap Message on SIM smartcard or 2G UICC

D.2.3 Access Method

SIM Commands Read Binary and Update Binary, as defined in [TS151.011], are used to access the Bootstrap Message.

D.2.4 Access Conditions

The Device is informed of the access conditions of the Bootstrap Message by evaluating the “private” and “modifiable” flags in the corresponding DODF-bootstrap files structure. When one of these flags is set cardholder verification is required. The CHV1 MUST be verified as defined in [TS151.011] when the “private” or “modifiable” flags are set.

Access conditions for files are proposed in the section D.4.

D.2.5 Requirements on the SIM or 2G UICC

To retrieve the Bootstrap Message from the SIM or 2G UICC, the Device MUST perform the following steps:

- Read EF (DIR) to evaluate the PKCS#15 application template and find the file identifier (and DF Path of the PKCS#15 DF),
- Select PKCS#15 DF (indirect selection), as defined in [TS151.011],
- Read ODF,
- Read DODF-bootstrap to locate the DM_Bootstrap file,
- Read the DM_Bootstrap file.

D.3 Bootstrap Message on UICC Activated in 3G Mode

D.3.1 Access to the file structure

To select the PKCS#15 application, the Device:

- MUST evaluate the PKCS#15 application template – i.e. PKCS#15 AID - present in the EF (DIR),
- MUST open a logical channel using UICC Command MANAGE CHANNEL as specified in [TS102.221],
- MUST select the PKCS#15 ADF using the PKCS#15 AID as parameter of the UICC Command SELECT, using direct application selection as defined in [TS102.221].

DM_Bootstrap file will be located under the PKCS#15 ADF.

D.3.2 Files Overview

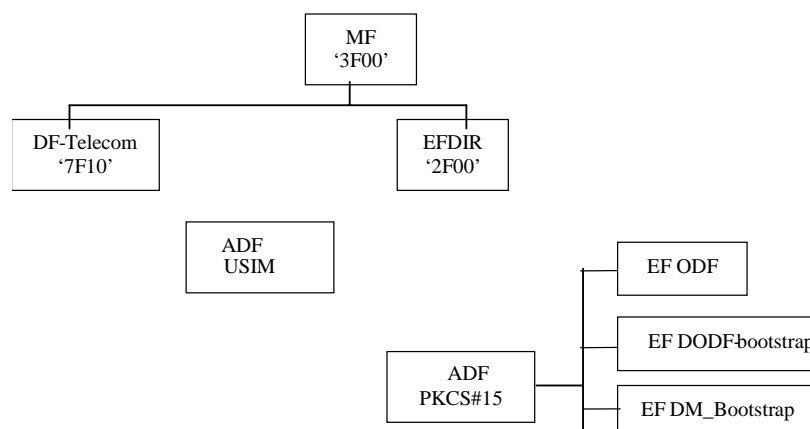


Figure 8: File structure for Bootstrap Message on 3G UICC

D.3.3 Access Method

UICC Commands Read Binary and Update Binary, as defined in [TS102.221], are used to access bootstrap data.

D.3.4 Access Conditions

The Device is informed of the access conditions of provisioning files by evaluating the “private” and “modifiable” flags in the corresponding DODF-bootstrap files structure.

In the case where one of the above mentioned flag is set, cardholder verification is required. The Device must evaluate the PIN references that must be verified as defined in [TS102.221] i.e. evaluate the FCP.

Access conditions for files are proposed in section D.4.

D.3.5 Requirements on the 3G UICC

To retrieve the Bootstrap Message from the 3G UICC, the Device MUST perform the following steps:

- Select PKCS#15 file structure as specified in D.3.1.
- Read ODF to locate the DODF-bootstrap,
- Read DODF-bootstrap to locate the DM_Bootstrap file,

- Read the DM_Bootstrap file

D.4 Files Description

All files defined are binary files as defined in [TS102.221]. These files are read and updated using SIM or UICSS Commands related to the application they belong to.

D.4.1 Object Directory File, EF ODF

The mandatory Object Directory File (ODF) ([PKCS#15], section 5.5.1) contains pointers to other EFs, each one containing a directory of PKCS#15 objects of a particular class (e.g. DODF-bootstrap). The File ID is specified in [PKCS#15]. The card issuer decides the file size. The EF (ODF) can be read but it MUST NOT be modifiable by the user.

In the case of SIM or UICC, the EF (ODF) is described below:

Identifier: default 0x5031, see [PKCS#15]	Structure: Binary	Mandatory
File size: decided by the card issuer	Update activity: low	
Access Conditions:		
READ	ALW	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	
Description		
See [PKCS#15]		

D.4.2 Bootstrap Data Object Directory File, EF DODF-bootstrap

This Data Object Directory File provisioning contains directories of provisioning data objects ([PKCS#15], section 6.7) known to the PKCS#15 application.

The File ID is described in the EF (ODF). The file size depends on the number of provisioning objects stored in the smartcard. Thus, the card issuer decides the file size.

Identifier: 0x6420, See ODF	Structure: Binary	Mandatory
File size: decided by the card issuer	Update activity: low	

Access Conditions:	
READ	ALW
or CHV1 (SIM, See section D.2)	
or Universal / application / Local PIN (UICC, See section D.3)	
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM
Description	
See hereafter and [PKCS#15]	

The EF (DODF-bootstrap) MUST contain information on provisioning objects:

- Readable label describing the provisioning document (`CommonObjectAttributes.label`). The ME could display this label to the user.
- Flags indicating whether the provisioning document is private (i.e., is protected with a PIN) and/or modifiable (`CommonObjectAttributes.flags`). The card issuer decides whether or not a file is private (it does not need to be if it does not contain any sensitive information)
- Object identifier indicating a DMbootstrap object and the type of the provisioning object (`CommonDataObjectAttributes.applicationOID`)
- Pointer to the contents of the provisioning document (`Path.path`)

The EF(DODF-bootstrap) MUST contain the types of provisioning documents (indicated using object identifiers) to be used by the ME. The Bootstrap type is described hereafter.

A dedicated OID is required and defined for each provisioning file:

- Bootstrap OID = { joint-isu-itu-t(2) international-organizations(23) wap(43) oma-dm(7) dm-bootstrap(1) }

The ME MUST use the OID to distinguish the DODF-bootstrap from any other DODF. The EF(DODF-bootstrap) can be read but it MUST NOT be modifiable by the user.

D.4.3 EF DM_Bootstrap

Only the card issuer can modify EF DM_Bootstrap

Setting all bytes to 'FF' initialises EF DM_Bootstrap.

Identifier: See DODF	Structure: Binary	Optional
File size: decided by the card issuer	Update activity: low	
Access Conditions: <p style="text-align: center;"> READ ALW or CHV1 (SIM, See section D.2) or Universal / application / Local PIN (UICC, See section D.3) </p> <p style="text-align: center;"> UPDATE ADM INVALIDATE ADM REHABILITATE ADM </p>		
Description		
Contains a Bootstrap Message		

Appendix E. DM Bootstrap Server discovery (Informative)

Discovery of the DM Bootstrap Server by the Device is an optional feature of OMA-DM. This technical specification specifies the following alternatives for the Device to deduce the FQDN (Fully Qualified Domain Name) of the DM Bootstrap Server.

1. The Device first obtains its domain name from the response that it receives for a DHCP query that includes the "Client FQDN" option, with an empty Domain Name field, as specified in [RFC4702] and [RFC4704]. It then prefixes the domain name with fixed string "OMADM-BootSrv" and issues a DNS Resource Record query, as specified in [RFC2782]. The structure of the query is as follows:

`_omadm-bootstrap._tcp.<Domain>`

2. The Device first obtains its domain name from the response that it receives for a DHCP query that includes the "Access Network Domain Name" option, as specified in [RFC5986]. It then prefixes the domain name with fixed string "OMADM-BootSrv" and issues a DNS Resource Record query, as specified in [RFC2782]. The structure of the query is as follows:

`_omadm-bootstrap._tcp.<Domain>`

The "omadm-bootstrap" service is registered with IANA and more information of this registration can be found at the following: <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>.

It needs to be noted that other alternatives are not precluded.