OMTP
USER EXPERIENCE

FUNCTIONAL REQUIREMENTS FOR REMOTE SERVICE PROVISIONING

VERSION:	OMTP Remote Service Provisioning Version 2_0, Release 2
STATUS:	Approved
DATE OF LAST EDIT:	27 January 2006
OWNER:	OMTP User Experience Group

CONTENTS

1 INTRODUCTION

1.1 DOCUMENT PURPOSE

The increasing complexity of mobile terminals presents a continuous challenge for mobile operators. New mobile terminals provide a wide range of new services including web browsing, data synchronisation, video streaming etc.

The number of parameters required to provision these services is increasing dramatically because of this increasing complexity.

Operators therefore wish to have a mechanism to provision mobile operator services parameters:

- At the point of manufacture.
- Automatically, when the terminal and the operator Smart Card are first paired.
- Automatically and Remotely, when settings or services need to be changed or updated.
- Automatically and Remotely, when a customer changes network operator but wishes to keep the same terminal.
- Manually and Remotely post sale, when a customer checks manually for updated settings.
- Automatically and Remotely, whenever the terminal's firmware is updated.

The terms 'Remote' and 'Remotely', as used throughout this document, mean the provisioning can take place:

- 'Over the Air' (OTA) with the terminal communicating to a provisioning server within the operator's network.
- 'Via a PC' when connected to a trusted server over the Internet using a PC (with suitable cable, Bluetooth or other type of link) as a conduit.
- Via the operator Smart Card, if it has been updated with related information.

The operator settings required to perform the provisioning will be stored in various locations, depending upon differing operator requirements, and transferred to the terminal in a number of ways. For example:

- Some operators will wish to configure all settings at the point of manufacture by providing the terminal vendor with a standard, generic list of settings in a format that can be used for all terminal makes and models.

- Some operators will store all provisioning settings on the Smart Card and require the terminal to read these settings from the Smart Card when the terminal and Smart Card are paired.
- Some operators will store all the provisioning settings on the Network and require the terminal to acquire these setting OTA from the network when the terminal registers to the network. Note: in this case, operators will:
  - preload their Smart Cards with their device management server connection settings, or
  - deliver the server connection settings OTA, or
  - require the terminal vendor to preload the server connection settings at the point of manufacture.
- Some operators will use a combination of all three methods listed above.

In all cases, it is critical that the interaction necessary for subscribers to perform the provisioning (alerts, questions, confirmations etc.) must be defined in a clear and optimal way in order to get the maximum acceptance rate.

Notes:

- The requirements for any particular service detailed in this document are only applicable if the target terminal supports the intended service.
- All the requirements in this document are applicable to both post-paid and pre-paid subscribers.
- It is essential that at any point during the provisioning process any user data stored on the terminal should not be overwritten, deleted, or uploaded without the user's consent.

An example of a user flow for remote provisioning is shown diagrammatically below in Figure 1:

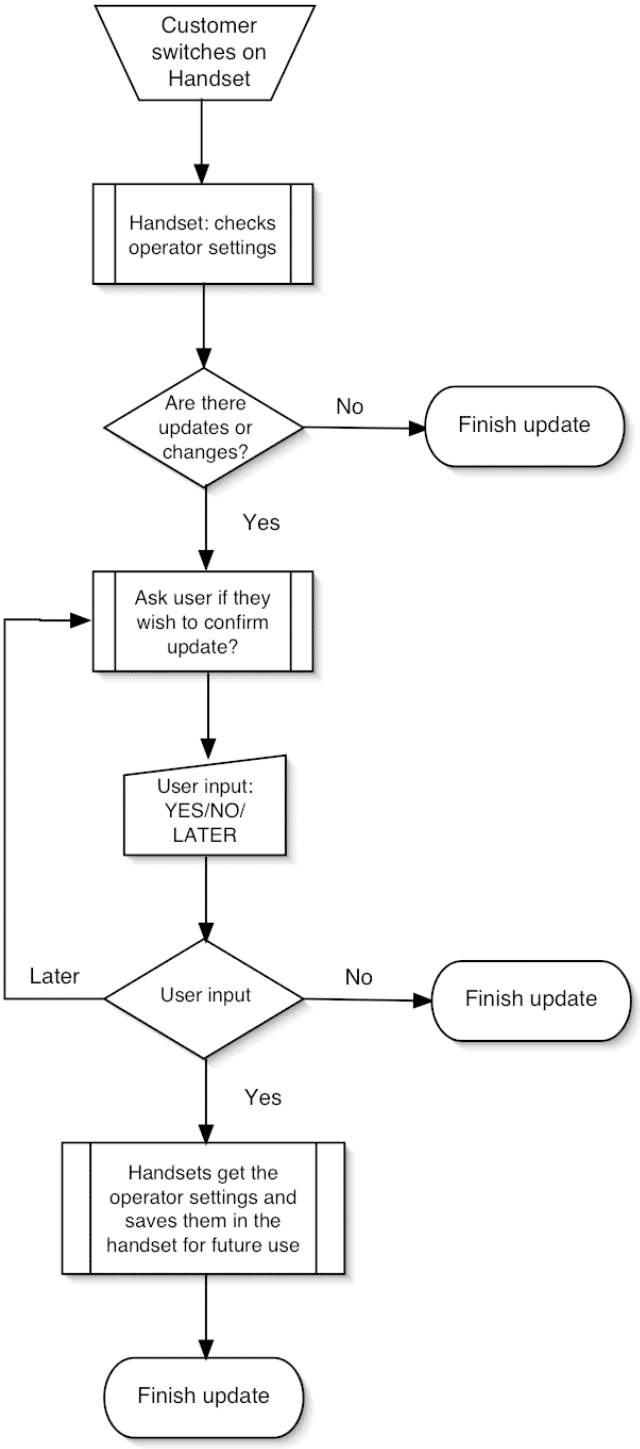

Figure 1: Example of a provisioning user flow (provided for information only).

1.2 INTENDED AUDIENCE

There are two main audiences for this specification:

- Other workstreams inside OMTP that will take these requirements as input.
- OMTP device implementers, i.e. the equipment and technology vendors that will be asked to create implementations of the OMTP platform.

1.3 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 [1].

- MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- MUST NOT: This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
- MAY: This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

The requirements within this document are uniquely identified using the following format:

- DM5X-Y###, where:
  - X refers to the device management level (“A”, ”B”, etc.).
  - Y refers to the requirement type (either “G” for a general requirement or “F” for a functional requirement).
  - ### is a number that identifies the requirement.

2 GENERAL REQUIREMENTS

The requirements in this section apply to all items contained within the document, unless otherwise specified in the relevant sections.

The requirements for any particular service detailed in this document are only applicable if the target terminal supports the intended service. Applicable service features may vary depending on the terminal category.

All the requirements in this document are applicable to both post-paid and pre-paid subscribers.

REQ. ID	REQUIREMENT
DM5A-G003	All the requirements in this document MUST be implemented securely within the terminal according to the security framework defined by the OMTP Application Security Project and Hardware Project Trusted Environment Task (forthcoming).
DM5A-G004	During the provisioning process, any user data (e.g. personal data such as the users' phonebook or calendar appointments) stored on the terminal MUST NOT be overwritten, deleted, or uploaded without user's consent.

3 SERVICES APPLICABLE TO REMOTE PROVISIONING

REQ. ID	REQUIREMENT
DM5A-F001	Operators MUST be able to provision WAP settings as specified in the OMA WAP specifications (see suggested parameters in Annex A) in a Consistent way (i.e. using either OMA CP or OMA DM technologies) across all terminals.
DM5A-F002	Operators MUST be able to provision MMS settings as specified in the OMA specifications (see suggested parameters in Annex A) in a Consistent way (i.e. using either OMA CP or OMA DM technologies) across all terminals.
DM5A-F003	Operators MUST be able to provision Web browser settings (see suggested parameters in Annex A) in a Consistent way (i.e. using either OMA CP or OMA DM technologies) across all terminals.
DM5A-F004	Operators MUST be able to provision streaming settings (see suggested parameters in Annex A) in a Consistent way (i.e. using either OMA CP or OMA DM technologies) across all terminals.
DM5A-F005	Operators MUST be able to provision email settings as specified in the SMTP, POP3 and IMAP specifications (see suggested parameters in Annex A) in a Consistent way (i.e. using either OMA CP or OMA DM technologies) across all terminals.
DM5A-F006	Operators MUST be able to provision device management settings as specified in the OMA DM specifications (see suggested parameters in Annex A) in a Consistent way (i.e. using either OMA CP or OMA DM technologies) across all terminals.
DM5A-F007	Operators MUST be able to provision data synchronisation settings as specified in the OMA Data Synchronisation specifications (see suggested parameters in Annex A) in a Consistent way (i.e. using either OMA CP or OMA DM technologies) across all terminals.

REQ. ID	REQUIREMENT
DM5A-F008	Operators MUST be able to provision presence and instant messaging settings as specified in the OMA Instant Messaging and Presence Service specifications (see suggested parameters in Annex A) in a Consistent way (i.e. using either OMA CP or OMA DM technologies) across all terminals.
DM5A-F009	Operators MUST be able to provision Push To Talk settings (see suggested parameters in Annex A) in a Consistent way (i.e. using either OMA CP or OMA DM technologies) across all terminals.
DM5A-F010	Operators MUST be able to provision WiFi settings as specified by the IEEE specifications (see suggested parameters in Annex A) in a Consistent way (i.e. using either OMA CP or OMA DM technologies) across all terminals.
DM5A-F011	Operators MUST be able to provision SIP settings (see suggested parameters in Annex A) in a Consistent way (i.e. using either OMA CP or OMA DM technologies) across all terminals.
DM5A-F012	Operators MUST be able to provision APN profiles (see suggested parameters in Annex A) in a Consistent way (i.e. using either OMA CP or OMA DM technologies) across all terminals.
DM5A-F034	Operators MUST be able to provision Operator applications and all applications that have a client server relationship with a server residing in the operator network.

4 FUNCTIONAL REQUIREMENTS RELATING TO THE UNDERLYING PROVISIONING PROCESS

REQ. ID	REQUIREMENT
DM5A-F013	An operator MUST be able to provision all of its services and settings on a terminal at the point of manufacture to provide the terminal vendor with a list of settings using data structures available in the standards referred by the OMTP Technology Agnostic Core Software Platform Device Management Enabler requirements [2] (e.g. OMA DM Profile or OMA CP Profile). The operator shall be able to provide the same list of settings in the same format to all terminal vendors and, vice versa, all operators shall use the same format.
DM5A-F014	An operator MUST be able to Automatically and Remotely provision the services on a terminal at the Point of Sale (i.e. in the store where the customer purchases the terminal).
DM5A-F015	An operator MUST be able to Automatically and Remotely provision the services on a terminal when a new Smart Card is inserted into the terminal.
DM5A-F016	An operator MUST be able to Automatically and Remotely change or update the configuration of services on existing terminals when new settings or services become available on the network.
DM5A-F017	The terminal MUST enable an operator to Automatically and Remotely provision services on a terminal when a customer changes network operator but wishes to keep the same terminal (i.e. provision a terminal that had operator X's settings with the new operator's settings).
DM5A-F020	For operators who store all their service provisioning data on their Smart Cards in a standardised format, the terminal MUST use this data for service provisioning, if it is available.
DM5A-F021	Operators who utilise OTA Remote provisioning may preload their Smart Cards with their device management server connection details. If these details are present on the Smart Card, the terminal MUST utilise these settings to complete full OTA device provisioning.

REQ. ID	REQUIREMENT
DM5A-F022	Service provisioning and configuration updates MUST not compromise other services on the terminal[1].
DM5A-F033	For Terminals which allow Operators to install new applications OTA, the Terminal MUST provide the new application with secure connectivity via an internal channel to the Device Management object tree in the Terminal, so that it can subsequently be managed OTA by the Operator. The Terminal MUST limit the new application to only access objects to which it is authorised. Typically, this would be the object created by the application.

[1] For example, if an operator makes an update to the WAP APN profile, other APN profiles, such as the Web browser APN profile, should not be affected by the update.

5 FUNCTIONAL REQUIREMENTS RELATING TO THE PROVISIONING USER EXPERIENCE

REQ. ID	REQUIREMENT
DM5A-F023	The operator MUST be able to choose, on a case-by-case basis for each update, to make the provisioning or configuration update of a terminal invisible to the user (i.e. to take place without the user's knowledge).
DM5A-F024	The operator MUST be able to choose, on a case-by-case basis for each update, to make the provisioning or configuration update of a terminal visible to the user.
DM5A-F025	When service provisioning or configuration updates are visible to the user, the operator MUST be able to request user confirmation.
DM5A-F026	When service provisioning or configuration updates are invisible, the user SHOULD not be prevented from using any of the services or applications on their terminal while updates are underway (if necessary, this could result in the configuration update being delayed until a feasible time).
DM5A-F027	When service provisioning or configuration updates are invisible to the user, any task that the user was performing when the update started SHOULD still be able to be completed successfully, e.g. if the user was composing a text message when a configuration update started, the user should still be able to send the text message successfully (if necessary, this could result in the configuration update being delayed until a feasible time).
DM5A-F028	Service provisioning and configuration updates MUST NOT require the user to restart or reboot the terminal.
DM5A-F029	When the operator has requested that the update is visible to the user, the operator MUST have the option to request that the terminal displays a message to indicate to the user that the provisioning or configuration process has finished.
DM5A-F030	An operator MUST be able to define whether the user is notified each time a connection to the OTA server is established.

REQ. ID	REQUIREMENT
DM5A-F031	The terminal MUST provide a function to allow the user to restore the service settings of the terminal back to its default factory settings.
DM5A-F032	When the operator has requested that the update is visible to the user, the operator MUST have the option to define whether audible feedback is given to the user when messages are displayed on the screen. The audible feedback MUST respect the current device profile.

6 DEFINITION OF TERMS

TERM	DESCRIPTION
AUTOMATICALLY	Meaning a process takes place without the user manually having to enter data via the terminal's keypad.
CONSISTENT	Being implemented in a common, coherent and uniform manner at all layers within the terminal (i.e. at the User Interface, Client and Transport layers).
POINT OF SALE	Location where the user buys the terminal.
REMOTE	Meaning that the provisioning can take place: • 'Over the Air' with the terminal communicating to a provisioning server within the operators network or communicating with the Smart Card after an over-the-air update, and • 'Via a PC', when connected to a trusted server over the Internet using a PC (with suitable cable, Bluetooth or other type of link) as a conduit.
REMOTELY	Meaning the that provisioning can take place: • 'Over the Air' with the terminal communicating to a provisioning server within the operators network or communicating with the Smart Card after an over-the-air update, and • 'Via a PC', when connected to it via a cable, Bluetooth or other type of link.
SMART CARD	The User Equipment incorporates a Smart Card being the trusted-by-operator module. The Smart Card contains a trusted-by-operator execution environment and a trusted-by-operator memory. The Smart Card is a tamper-resistant device. The Smart Card communicates with the UE through its interface. The Smart Card is issued by the operator as: • Operator security module • User Identification module The Smart Card could be a SIM (GSM), R-UIM (CDMA) or an application as the USIM (UMTS) on the UICC platform.

7 ABBREVIATIONS

ABBREVIATION	DESCRIPTION
APN	Access Point Node
CHAP	Challenge-Handshake Authentication Protocol
CP	Client Provisioning
DM	Device Management
DNS	Domain Name System
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
MMS	Multimedia Messaging Service
OMA	Open Mobile Alliance
OMTP	Open Mobile Terminal Platform
OTA	Over The Air
PAP	Password Authentication Procedure
PDP	Packet Data Protocol
POP3	Post Office Protocol 3
R-UIM	Removable User Identity Module
SC	Smart Card
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
UDP	User Datagram Protocol
UICC	Universal Integrated Circuit Card

ABBREVIATION	DESCRIPTION
UMTS	Universal Mobile Telecommunications Service
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module or User Services Identity Module
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy

8 REFERENCED DOCUMENTS

NO.	DOCUMENT	AUTHOR	DATE
1	RFC2119 (http://rfc.net/rfc2119.html)	RFC	March 1997
2	"OMTP Software: Device Management Enabler" Version 1_0, Release 1_0	OMTP	December 2005

ANNEX A: SUGGESTED PARAMETERS

This annex describes some suggested parameters for each service that might be adopted by OMTP in a device management implementation that would enable configuration in a consistent way across all the range of terminals.

Please note that the configuration parameters in this annex ***do not*** constitute requirements.

APN PROFILE CONFIGURATION

PARAMETER NAME	DESCRIPTION
APN PROFILE NAME	Identifier of the APN profile.
APN ADDRESS	Address of the access point used for this connection.
APN USER	User Name to log in the APN.
APN PASSWORD	Password associated with the user name.
APN AUTHENTICATION TYPE	Type of authentication required on the APN (PAP, CHAP).

MMS CONFIGURATION

PARAMETER NAME	DESCRIPTION
PROFILE NAME	Identifier of the MMS connection.
AUTO RETRIEVE	Determine whether MMS must be retrieved automatically upon notification.
SERVER NAME	MMS Server URL.
MAXIMUM SIZE	The maximum size over which MMSs are not sent or received.
APN PROFILE	Identifier of the APN profile to be used.
PRIMARY PROXY ADDRESS	Address of the primary proxy.
PRIMARY PROXY PORT	Port of the primary proxy.
SECONDARY PROXY ADDRESS	Address of the secondary proxy.
SECONDARY PROXY PORT	Port of the secondary proxy.

WAP CONFIGURATION

PARAMETER NAME	DESCRIPTION
PROFILE NAME	Identifier of the WAP connection.
APN PROFILE	Identifier of the APN profile to be used.
PRIMARY PROXY ADDRESS	Address of the primary proxy.
PRIMARY PROXY PORT	Port of the primary proxy.
SECONDARY PROXY ADDRESS	Address of the secondary proxy.
SECONDARY PROXY PORT	Port of the secondary proxy.
DATA BEARER	The type of data bearer to be used.

WEB BROWSER CONFIGURATION

PARAMETER NAME	DESCRIPTION
PROFILE NAME	Identifier of the browser connection.
APN PROFILE	Identifier of the APN profile to be used.
SECURE CONNECTION	Determines whether secure connection is used or not.
PRIMARY DNS	Primary DNS address used to resolve a domain name.
SECONDARY DNS	Secondary DNS address used to resolve a domain name.
PRIMARY PROXY ADDRESS	Address of the primary proxy.
PRIMARY PROXY PORT	Port of the primary proxy.
SECONDARY PROXY ADDRESS	Address of the secondary proxy.
SECONDARY PROXY PORT	Port of the secondary proxy.
PROXY USER	User Name to log into the proxy.

PARAMETER NAME	DESCRIPTION
PROXY PASSWORD	Password associated with the proxy user name.
DATA BEARER	The type of data bearer to be used.
LINGER	The period of inactivity (in seconds) before an application 'times out' and releases PDP context.

STREAMING CONFIGURATION

PARAMETER NAME	DESCRIPTION
PROFILE NAME	Identifier of the streaming connection.
STARTPAGE	Streaming connection home page.
APN PROFILE	Identifier of the APN profile to be used.
PRIMARY DNS	Primary DNS address used to resolve a domain name.
SECONDARY DNS	Secondary DNS address used to resolve a domain name.
PRIMARY PROXY ADDRESS	Address of the primary proxy.
PRIMARY PROXY PORT	Port of the primary proxy.
SECONDARY PROXY ADDRESS	Address of the secondary proxy.
SECONDARY PROXY PORT	Port of the secondary proxy.
LOWEST UDP	Minimum UDP number used for media data traffic.
HIGHEST UDP	Maximum UDP number used for media data traffic.
LINGER	The period of inactivity (in seconds) before an application 'times out' and releases PDP context.

EMAIL CONFIGURATION

PARAMETER NAME	DESCRIPTION
PROFILE NAME	Identifier of the email account.
APN PROFILE	Identifier of the APN profile to be used.
PRIMARY DNS	Primary DNS address used to resolve a domain name
SECONDARY DNS	Secondary DNS address used to resolve domain name.
PRIMARY PROXY ADDRESS	Address of the primary proxy.
PRIMARY PROXY PORT	Port of the primary proxy.
SECONDARY PROXY ADDRESS	Address of the secondary proxy.
SECONDARY PROXY PORT	Port of the secondary proxy.
PROXY USER	User name to log into the proxy.
PROXY PASSWORD	Password associated with the proxy user name.
INCOMING SERVER	Host name of the incoming server.
INCOMING SERVER PORT	Port of the incoming server.
OUTGOING SERVER	Host name of the sending server.
OUTGOING SERVER PORT	Port of the outgoing server.
RECEIVING PROTOCOL	Remote mailbox protocol.
EMAIL ADDRESS	User email's address.
ACCOUNT NAME	User ID for the email account.
PASSWORD	Password for the email account.
SECURE CONNECTION	Defines whether a secure connection is used or not.

PARAMETER NAME	DESCRIPTION
SMTP ID	User identification for the SMTP server.
SMTP PASSWORD	Password for the SMTP server.
MAXIMUM SIZE	The maximum size for emails. Emails larger than this size are not sent or received.
HEADER ONLY	Defines whether a complete email message or just the email header is retrieved.
RETRIEVE ATTACHMENTS	Defines whether attachments are retrieved automatically together with the message body.
AUTOCHECK	Defines the conditions under which the client will automatically check for new email messages (i.e. never, always or on home network only).
AUTOCHECK INTERVAL	Defines how often (in minutes) the client checks for new email messages.
LEAVE MESSAGES ON SERVER	Defines whether messages should be left on the incoming server upon retrieval.

DEVICE MANAGEMENT CONFIGURATION

PARAMETER NAME	DESCRIPTION
PROFILE NAME	Displayable name of the Device Management account.
DM SERVER ADDRESS	Device Management server address.
DM SERVER PORT	Device Management server port.
DM AUTHENTICATION TYPE	Authentication scheme used in the Device Management Server.
CLIENT USER NAME	Client User name.
CLIENT PASSWORD	Client Password.

PARAMETER NAME	DESCRIPTION
SERVER USER NAME	Identification of the DM server.
SERVER PASSWORD	Password that the server will use to authenticate itself to the client.
APN PROFILE	Identifier of the APN profile to be used.
PRIMARY DNS	Primary DNS address used to resolve domains name.
SECONDARY DNS	Secondary DNS address used to resolve domains name.
PRIMARY PROXY ADDRESS	Address of the primary proxy.
PRIMARY PROXY PORT	Port of the primary proxy.
SECONDARY PROXY ADDRESS	Address of the secondary proxy.
SECONDARY PROXY PORT	Port of the secondary proxy.
PROXY USER	User name to log in the proxy.
PROXY PASSWORD	Password associated with the proxy user name.

DATA SYNCHRONISATION CONFIGURATION

PARAMETER NAME	DESCRIPTION
PROFILE NAME	Connection displayable name.
DS SERVER ADDRESS	Data synchronisation server address.
DS SERVER PORT	Data synchronisation server port number.
CLIENT USER NAME	Data synchronisation server user name.
CLIENT PASSWORD	Data synchronisation server password.
DATABASE MEDIA CONTENT	Identify the supported media content of the database.

PARAMETER NAME	DESCRIPTION
LOCAL DATABASE URI	Relative of absolute URI of the local database.
REMOTE DATABASE URI	Relative of absolute URI of the remote database.
APN PROFILE	Identifier of the APN profile to be used.
PRIMARY DNS	Primary DNS address used to resolve a domain name.
SECONDARY DNS	Secondary DNS address used to resolve a domain name.
PRIMARY PROXY ADDRESS	Address of the primary proxy.
PRIMARY PROXY PORT	Port of the primary proxy.
SECONDARY PROXY ADDRESS	Address of the secondary proxy.
SECONDARY PROXY PORT	Port of the secondary proxy.
PROXY USER	User name to log in the proxy.
PROXY PASSWORD	Password associated with the proxy user name.

PRESENCE AND INSTANT MESSAGING CONFIGURATION

PARAMETER NAME	DESCRIPTION
PROFILE NAME	Presence profile displayable name.
PRESENCE SERVER ADDRESS	Presence server address.
PRESENCE USER NAME	Presence user name.
PRESENCE PASSWORD	Presence password.
APN PROFILE	Identifier of the APN profile to be used.
PRIMARY DNS	Primary DNS address used to resolve a domain name.

PARAMETER NAME	DESCRIPTION
SECONDARY DNS	Secondary DNS address used to resolve a domain name.
PRIMARY PROXY ADDRESS	Address of the primary proxy.
PRIMARY PROXY PORT	Port of the primary proxy.
SECONDARY PROXY ADDRESS	Address of the secondary proxy.
SECONDARY PROXY PORT	Port of the secondary proxy.
PROXY USER	User name to log in the proxy.
PROXY PASSWORD	Password associated with the proxy user name.

PUSH TO TALK CONFIGURATION

PARAMETER NAME	DESCRIPTION
PROFILE NAME	Push to Talk profile displayable name.
POC SERVER ADDRESS	Push to Talk server address URI (SIP server URI).
POC USER NAME	User name to log in the Push to Talk server.
POC PASSWORD	Password for the Push to Talk server.
POC PORTAL	Address of the Push to Talk portal (SIP portal).
APN PROFILE	Identifier of the APN profile to be used.
PRIMARY DNS	Primary DNS address used to resolve a domain name.
SECONDARY DNS	Secondary DNS address used to resolve a domain name.
PRIMARY PROXY ADDRESS	Address of the primary proxy.
PRIMARY PROXY PORT	Port of the primary proxy.

PARAMETER NAME	DESCRIPTION
SECONDARY PROXY ADDRESS	Address of the secondary proxy.
SECONDARY PROXY PORT	Port of the secondary proxy.
PROXY USER	User name to log in the proxy.
PROXY PASSWORD	Password associated with the proxy user name.

WIFI CONFIGURATION

PARAMETER NAME	DESCRIPTION
CONNECTION PROFILE NAME	WiFi connection displayable name.
NETWORK MODE	Infrastructure mode (Ad hoc mode or Any).
AUTOMATICALLY CONNECT	Yes or No.
SECURITY MODE	Security required in the Wireless network (none, WEP, WPA, WPA-PSK).
NETWORK KEY LENGTH	Length of the WEP key.
NETWORK KEY TYPE	WEP key format (Hexadecimal or ASCII).
NETWORK KEY DATA	Data that defines the WEP key.
DATA ENCRYPTION	Disabled, WEP, TKIP or AES.
AUTORETRIEVE IP ADDRESS	Indicates if the IP address should be retrieved automatically from the server.
IP ADDRESS	IP address used (only if IP auto retrieve is not used).
DEFAULT GATEWAY	Default gateway (only if IP auto retrieve is not used).
NETWORK MASK	IP network mask (only if IP auto retrieve is not used).
AUTORETRIEVE DNS	Indicates if the DNS addresses should be retrieved automatically from the server.

PARAMETER NAME	DESCRIPTION
PRIMARY DNS	Primary DNS address used to resolve domains name (only if auto retrieve DNS is not used).
SECONDARY DNS	Secondary DNS address used to resolve domains name (only if auto retrieve DNS is not used).
PRIMARY PROXY ADDRESS	Address of the primary proxy.
PRIMARY PROXY PORT	Port of the primary proxy.
SECONDARY PROXY ADDRESS	Address of the secondary proxy.
SECONDARY PROXY PORT	Port of the secondary proxy.
PROXY USER	User Name to log in the proxy.
PROXY PASSWORD	Password associated with the proxy user name.

SIP CONFIGURATION

PARAMETER NAME	DESCRIPTION
CONNECTION PROFILE NAME	Connection profile displayable name.
APN PROFILE	Identifier of the APN profile to be used.
SIP PROFILE NAME	SIP profile displayable name.
SIP PROXY ADDRESS	Address of the SIP proxy.
SIP PROXY PORT	Port of the SIP proxy.
SIP REGISTRATION SERVER ADDRESS	Address of the SIP registration server.
SIP REGISTRATION SERVER PORT	Port of the SIP registration server.
AUTHENTICATION TYPE	Type of authentication to be used.
DISPLAY NAME	User displayable name.

PARAMETER NAME	DESCRIPTION
SIP URI	URI reporting the registration name.
SIP PASSWORD	Password for the registration.
SIP REALM	SIP domain.
SIP VERSION	SIP version to be used.
SIP MODE	Stack to be used (IETF/IMS).
ALWAYS ON	Indication if the connection should be kept always active.