OMA DM Client Functional Requirements for SIM OTA Devices

Version 2.0

March 20th, 2019

Bret Sumner

Table Of Contents

Document History

This section is intended to be an aid to the reader. It is not meant to be a comprehensive list of all changes from previous versions. The reader is encouraged to review the entire document.

Revision	Date	Author	Comments
1.0	Jan 13, 2017	Bret Sumner	New Specification Release
1.1	Jun 23, 2017	Bret Sumner	Added: OMA-SIMOTA-00281, OMA-SIMO-TA-00280 Updated: OMA-SIMOTA-00063, OMA-SIMO-TA-00067, OMA-SIMOTA-00120, OMA-SIMO-TA-00121, OMA-SIMOTA-00122, OMA-SIMO-TA-00147, OMA-SIMOTA-00161, OMA-SIMO-TA-00179, OMA-SIMOTA-00180, OMA-SIMO-TA-00181, OMA-SIMOTA-00182, OMA-SIMO-TA-00183, OMA-SIMOTA-00184, OMA-SIMO-TA-00185, OMA-SIMOTA-00186, OMA-SIMO-TA-00187, OMA-SIMOTA-00220, OMA-SIMO-TA-00263, OMA-SIMOTA-00264, OMA-SIMO-TA-00266, OMA-SIMOTA-00269, Deprecated: OMA-SIMOTA-00031, OMA-SIMO-TA-00116, OMA-SIMOTA-00201
1.2	Nov 1, 2017	Bret Sumner	Added: OMA-SIMOTA-00305, OMA-SIMO-TA-00306, OMA-SIMOTA-00304, OMA-SIMO-TA-00282, OMA-SIMOTA-00283, DM-SIMO-TA-00307, OMA-SIMOTA-00284, OMA-SIMO-TA-00285, OMA-SIMOTA-00286, OMA-SIMO-TA-00287, OMA-SIMOTA-00288, OMA-SIMO-TA-00289, OMA-SIMOTA-00290, OMA-SIMO-TA-00291, OMA-SIMOTA-00292, OMA-SIMO-TA-00293, OMA-SIMOTA-00294, OMA-SIMO-TA-00295, OMA-SIMOTA-00296, OMA-SIMO-TA-00297, OMA-SIMOTA-00298, OMA-SIMO-TA-00299, OMA-SIMOTA-00300, OMA-SIMO-TA-00303, OMA-SIMOTA-00302, OMA-SIMO-TA-00301 Updated: OMA-SIMOTA-00078, OMA-SIMO-TA-00141, OMA-SIMOTA-00143, OMA-SIMO-TA-00144, OMA-SIMOTA-00145, OMA-SIMO-TA-00150, OMA-SIMOTA-00156, OMA-SIMO-TA-00157, OMA-SIMOTA-00158, OMA-SIMO-TA-00160, OMA-SIMOTA-00280, OMA-SIMO-TA-00235, OMA-SIMOTA-00234, OMA-SIMO-TA-00237, OMA-SIMOTA-00239, OMA-SIMO-TA-00242, OMA-SIMOTA-00248, OMA-SIMO-TA-00236, OMA-SIMOTA-00238, OMA-SIMO-TA-00240, OMA-SIMOTA-00241, OMA-SIMO-TA-00043, OMA-SIMOTA-00255, OMA-SIMO-TA-00278

Revision	Date	Author	Comments
			Deprecated: OMA-SIMOTA-00017, OMA-SIMO-TA-00112
1.3		Bret Sumner	Added: OMA-SIMOTA-00307, OMA-SIMO-TA-00308, OMA-SIMOTA-00309, OMA-SIMO-TA-00310, OMA-SIMOTA-00311, OMA-SIMO-TA-00312, OMA-SIMOTA-00313, OMA-SIMO-TA-00314 Updated: OMA-SIMOTA-00157, OMA-SIMO-TA-00096, OMA-SIMOTA-00029, OMA-SIMO-TA-00057, OMA-SIMOTA-00276, OMA-SIMO-TA-00108, OMA-SIMOTA-00102, OMA-SIMO-TA-00225
1.4		Susan Long, Bret Sumner	removed Module device type from OMA-SIMOTA-00203, OMA-SIMOTA-00204 Added: OMA-SIMOTA-00316, OMA-SIMO-TA-00315 Updated: OMA-SIMOTA-00307, OMA-SIMO-TA-00308, OMA-SIMOTA-00309, OMA-SIMO-TA-00310, OMA-SIMOTA-00311, OMA-SIMO-TA-00312, OMA-SIMOTA-00313, OMA-SIMO-TA-00233 Deprecated: OMA-SIMOTA-00163, OMA-SIMO-TA-00164, OMA-SIMOTA-00165, OMA-SIMO-TA-00166
1.5	9-14-18	Bret Sumner	Added: OMA-SIMOTA-00318, OMA-SIMO-TA-00319 Updated: Changed Requirement ID DM-SIMO-TA-00307 to OMA-SIMOTA-00317
2.0	11-30-18	Bret Sumner	Removed Open Market from the Category tag for all requirements. Added: OMA-SIMOTA-00319 Updated: OMA-SIMOTA-00264, OMA-SIMO-TA-00072, OMA-SIMOTA-00097, OMA-SIMO-TA-00102, OMA-SIMOTA-00121, OMA-SIMO-TA-00252, OMA-SIMOTA-00263, OMA-SIMO-TA-00270, OMA-SIMOTA-00315, OMA-SIMO-TA-00220, OMA-SIMOTA-00310, OMA-SIMO-

Revision	Date	Author	Comments
			TA-00005, OMA-SIMOTA-00011, OMA-SIMO-TA-00306, OMA-SIMOTA-00020, OMA-SIMO-TA-00127 Deprecated: OMA-SIMOTA-00077, OMA-SIMO-TA-00103, OMA-SIMOTA-00104, OMA-SIMO-TA-00142, OMA-SIMOTA-00128, OMA-SIMO-TA-00129, OMA-SIMOTA-00130, OMA-SIMO-TA-00167, OMA-SIMOTA-00168, OMA-SIMO-TA-00169, OMA-SIMOTA-00170, OMA-SIMO-TA-00171, OMA-SIMOTA-00172, OMA-SIMO-TA-00173, OMA-SIMOTA-00174, OMA-SIMO-TA-00175, OMA-SIMOTA-00176, OMA-SIMO-TA-00177, OMA-SIMOTA-00178, OMA-SIMO-TA-00196, OMA-SIMOTA-00197, OMA-SIMO-TA-00198, OMA-SIMOTA-00199, OMA-SIMO-TA-00200, OMA-SIMOTA-00188, OMA-SIMO-TA-00179, OMA-SIMOTA-00189, OMA-SIMO-TA-00180, OMA-SIMOTA-00190, OMA-SIMO-TA-00181, OMA-SIMOTA-00194, OMA-SIMO-TA-00195, OMA-SIMOTA-00182, OMA-SIMO-TA-00191, OMA-SIMOTA-00183, OMA-SIMO-TA-00184, OMA-SIMOTA-00185, OMA-SIMO-TA-00186, OMA-SIMOTA-00187, OMA-SIMO-TA-00192, OMA-SIMOTA-00193, OMA-SIMO-TA-00265, OMA-SIMOTA-00266, OMA-SIMO-TA-00267, OMA-SIMOTA-00269

Preface

Audience:

The specification is written primarily for the implementation of an OMA-DM client on mobile devices. All devices or products that use Sprint's mobile networks are required to support this specification. Such products include but are not limited to:

• Mobile broadband data cards with host-based connection manager such as SmartView and mobile broadband devices using a host-less connection manager
• Smart phones (Windows Mobile, Android, Linux, etc.)
• Embedded modules (telemetry, GPS, laptops, etc.)
• Multi-mode devices that include LTE, in addition to CDMA
• All wholesale devices that operate on Sprint's mobile networks
• All Prepaid devices
• All other devices that use the OMA-DM infrastructure

Target Device Types: Smartphone

Target Device Categories: Cat1

Distribution Rights:

Acronyms

CIDC	Client Initiated Device Configuration
CSIM	CDMA Subscriber Identity Module: A UICC that includes CDMA provisioning information
Device NAI	The factory default MIP profile formerly known as slot-0 (includes NAI, password and HA values)
FOTA	Firmware Over The Air (deprecated term synonymous with FUMO)
FUMO	Firmware Update Management Object
HFA	Hands-Free Activation
HMAC	Refers to syncml:auth-MAC authentication in the context of this specification
LSK	The left soft key button on the device
LTE	Long Term Evolution
MBB	Mobile Broadband
MIP	Mobile Internet Protocol
MO	Management Object
MSL	Master Subsidy Lock Code
NIDC	Network Initiated Device Configuration
OMA-DM	Open Mobile Alliance Device Management (see http://www.openmobilealliance.org)
Proprietary FOTA	A custom over-the-air process for upgrading device firmware that does not comply with Sprint's FUMO requirements
RSK	The right soft key button on the device
SIM	Subscriber Identity Module: obsolete term. See UICC instead.

UE	User Equipment: Another name for a device, differentiated from the UICC
UICC	Universal Integrated Circuit Card: another name for the 4G SIM component
Vision NAI	The MIP profile information programmed during activation

Terminology and Conventions

Conventions:

Requirement Identifier:

- Each requirement will have a unique ID
- Each ID will consist of three letters for document type, dash, three letters for GTR key, dash, and 5 numbers for requirement ID
- Example: GTR-XXX-00056
  - GTR indicates Global Terminal Requirements
  - XXX indicates the GTR key
  - 00056 indicates the requirement number

Priority:

- Must - These requirements are mandatory. Waivers are typically not accepted for these items unless previously defined within the GTR.
- Should - These requirements are expected but may be waived on a case by case basis.
- Optional - These requirements are not required but typically enhance the overall customer experience. Implementation is recommended.

Waivers:

- Sectional Waiver - Defines the conditions required for the waiver to apply for an entire section.
- Requirement Waiver - Defines the conditions required for the waiver to apply to a particular requirement only.

WAIVER: Represents a requirement waiver.

References:

[DM Standard]	OMA-TS-DM_StdObj-V1_2-20070209-A.pdf
[DM RepPro]	OMA-TS-DM_RepPro-V1_2-20070209-A.pdf
[DL OTA]	OMA-Download-OTA-v1_0-20020620-p
[DM FUMO]	OMA-TS-DM-FUMO-V1_0-20050927-D.doc
[DM DDF]	OMA-SUP-dtd_dm_ddf-V1_2-20070209-A.dtd
[DM Protocol]	OMA-TS-DM_Protocol-V1_2-20070209-A.pdf
[DM Notification]	OMA-TS-DM_Notification-V1_2-20070209-A.pdf

1 OMA DM Client Bootstrapping

OMA-SIMOTA-00001

The OMA DM client must support the OMA DM 1.2 Standard.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00002

The DDF nodes must not be view-able or editable by the user through the keypad, AT commands or any other tools.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00003

Windows mobile devices are permitted to use the ./SyncML/DMS management object in lieu of the DMAcc MO.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00305

The OMA DM client must NEVER enable Mobile Data if it has been disabled by the user.

Priority: Must

Category: Cat1

Device: Smartphone

1.1 Factory Bootstrapping Algorithm

OMA-SIMOTA-00004

The following algorithm must be used by the handset OEM to generate the credentials that are used between the OMA-DM client and the OMA-DM server. These credentials are to be generated at the time of manufacture and stored into the device prior to the device shipment to Sprint.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00005

The parameter values to the algorithm below are:
The “equip” variable is the UPPERCASE hexadecimal ESN ~~or~~/ MEID or the IMEI of the device
The “server” variable is the serverID of the OMA-DM server
The “secret” variable is a shared secret String token

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00006

Pseudo-code for hash generation:

```
function f(a, b, s) returns String {
       x = a + b + s (String concatenation)
       convert x to byte array
       String digest = new String ( B64(MD5(x)) )
       replace all '+' characters with 'm' (lowercase)
       replace all '/' characters with 'f' (lowercase)
       remove all trailing '=' signs
       return digest
}cvn tzb
```

The digest String returned will be exactly 22 characters long in printable ASCII.

Test Example
equip equals “A000001A2B3C4F”
server equals “sprint”
secret equals “foobar”
f(equip, server, secret) returns “cWLvU1I8HV2wbaZJhLsNUw” and is stored in: ./DMAcc/AppAuth/clientAuth/AAuthSecret.

f(server, equip, secret) returns “5bptxBBw8lGxZTrOVb96KQ” and is stored in: ./DMAcc/AppAuth/serverAuth/AAuthSecret.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00007

The following assertion can be used to validate the Base64 encoding and MD5 hash:
B64(MD5(“foobar”)) is equal to “OFj2IjCsPJFfMAxmQxLGPw==”

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00008

The server ID (./DMAcc/ServerID) is “sprint”. The shared secret token is “dmsecret@sprint”.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00009

The client password (./DMAcc/AppAuth/<clientAuth>/AAuthSecret) must be calculated with the algorithm above as: f(equip, server, secret).

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00010

The initial client nonce (./DMAcc/AppAuth/<clientAuth>/AAuthData) must be B64("12345") which computes to: "MTIzNDU=".

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00011

The client user name (./DMAcc/AppAuth/<clientAuth>/AAuthName) must be the UPPERCASE hexadecimal ESN ~~or/~~ MEID or the IMEI of the device.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00012

The server password (./DMAcc/AppAuth/<serverAuth>/AAuthSecret) must be calculated with the algorithm above as: f(server, equip, secret).

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00013

The initial server nonce (./DMAcc/AppAuth/<serverAuth>/AAuthData) must be B64("12345") which computes to: "MTIzNDU=".

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00014

The server user name (./DMAcc/AppAuth/<serverAuth>/AAuthName) must be the same as the server ID value in ./DMAcc/ServerID.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00015

The device must not allow the credentials to be viewed or changed by the user or over the air.

Priority: Must

Category: Cat1

Device: Smartphone

1.2 Configuring the OMA DM Client for other Environments

OMA-SIMOTA-00016

If the device OEM provides any hidden command to edit the ./DMAcc nodes, the command must be disabled before final launch software is provided. If the device OEM provides this command, it must require the MSL before displaying or editing the values.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00306

The OMA DM client MUST support the table found ~~here~~ in the OMA DM / FUMO EAP for connecting the the various OMA servers. It must be statically populated for each device and the settings must not be generated on the fly. For example, the ./DMAcc/ AppAuth/clientAuth/AAuthSecret and ./DMAcc/AppAuth/serverAuth/AAuthSecret values must only be set when the device is manufactured and not updated later.

Priority: Must

Category: Cat1

Device: Smartphone

2 OMA DM Device Configuration

2.1 OMA-DM Session Details

This section describes how the OMA-DM Client establishes a connection and executes a session with the Sprint OMA-DM server. These requirements apply to all sessions with the server, both client-initiated and network-initiated.

OMA-SIMOTA-00018

The OMA DM client must support a <MaxObjSize> of at least 50KB.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00019

The client must establish the management session using the “Package 1” format defined in the [DM RepPro] standard.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00202

The device must display an error if the management session terminates abnormally, per the [OMA-DM Session Details] section.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00020

The client must support syncml:auth-MAC (“HMAC”) authentication. See the ./DMAcc/AAuthPref node in the OMA DM DDF Requirements for SIM OTA Devices GTR ~~the DDF reference [Sprint DDF]~~ and ~~Sprint PRI~~ GTR-OMADM-GSS for more information..

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00021

The client shall support the management session commands from Table 1: Supported Commands as defined in the representation protocol [DM RepPro]:

Command	Description
REPLACE	Change the value of data in a leaf node
GET	Query the content of a leaf node or list the children of an interior node
EXEC	Execute a native command linked to a node or leaf

Table 1: Supported Commands

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00022

The client must perform all management commands as instructed by the server.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00089

The device shall return a "404 error" to the server when instructed to perform an operation on a node that does not exist.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00023

The client must not skip commands or modify commands through evaluation of the new or previous values. For example, if the server replaces a node with the same value the client must perform the action completely and neither skip it nor return an error.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00090

The device shall be compliant with WB_XML and support the binary (bin) data type with a MIME type of application/octet-stream.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00024

The client must not apply any business logic to determine whether or not to perform any command(s). Instead the client must perform all management commands as specified in the management session.

Priority: Must

Category: Cat1

Device: Smartphone

2.2 Session Establishment

Sprint allows connections to the OMA-DM server using multiple network paths. It is possible to connect using both the factory default Device NAI (formerly known as slot-0 NAI) and also the Vision NAI (formerly known as slot-1 NAI) on the CDMA network. The client can also connect via Wifi, LTE, and CDMA networks. The clients are expected to follow the new connection rules stated in this section and throughout the document, using the Vision NAI on CDMA.

OMA-SIMOTA-00025

The client shall primarily use the values in the ./DMAcc MO to establish the management session with the DM Server.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00026

When directed, the device must attempt to connect to the OMA-DM server using the data network it is currently connected to.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00027

In the case where multiple network bearers are available and the device is not actively connected to anything, it must attempt to connect to OMA-DM in the following preference order:

Wifi -> LTE -> eHRPD -> CDMA

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00028

The user may always cancel or abort a DM session by pressing the [END] key or by pressing the designated “cancel” soft key or button. The session must also be canceled if the user presses the “Emergency Call” button on an OMA HFA UI screen.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00029

The DM session MUST NOT be canceled by opening/closing the flip or sliding a device open/closed.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00030

The DM session MUST NOT be canceled by pressing the “Home” or “Back” soft key or button.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00032

If the device is not connected to Wifi or LTE and the user has disabled data access over the Mobile network the device must NOT allow the OMA-DM Client to connect on CDMA.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00033

During client-initiated transactions, if the session fails for any reason the client shall display the error to the user interface and MUST NOT retry.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00036

The session establishment requirements outlined herein apply to both home and roaming networks. This includes International roaming.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00037

If the device is in roaming coverage and Data Roaming is disabled, the OMA DM client must not start a session.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00038

The client must perform a DNS query using the value in the ./OMADM/ProxyAddr node when starting a session with the OMA DM server.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00039

The client MUST include a Replace for the ./DevDetail/SwV in all MsgID 1 messages to the server.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00307

The client MUST include a Replace for the ./DevInfo/Bearer in all MsgID 1 messages to the server. The content of this node must be the network type the device is using for the OMA session.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00308

The client MUST include a Replace for the ./DevInfo/Ext/InsertedUICC/ICCID in all MsgID 1 messages to the server. The content of this node must be the ICCID on the SIM currently inserted in the active SIM slot/profile of the device.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00309

The client MUST include a Replace for the ./DevInfo/Ext/InsertedUICC/LTEIMSI in all MsgID 1 messages to the server. The content of this node must be the LTE IMSI from the SIM currently inserted in the active SIM slot/profile of the device.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00310

The client MUST include a Replace for the ./DevInfo/Ext/InsertedUICC/GID1 in all MsgID 1 messages to the server. The content of this node must be the USIM GID1 from the SIM currently inserted in the active SIM slot/profile of the device and must be in HEX format.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00311

The client MUST include a Replace for the ./DevInfo/Ext/VoLTEEnabled in all MsgID 1 messages to the server. The content of this node must be the current user enablement setting for VoLTE. If the user has enabled the service, the value for this node must be '1'. If the user has disabled the service, the value for this node must be '0'.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00312

The client MUST include a Replace for the ./DevInfo/Ext/VoWifiEnabled in all MsgID 1 messages to the server. The content of this node must be the current user enablement setting for VoWifi. If the user has enabled the service, the value for this node must be '1'. If the user has disabled the service, the value for this node must be '0'.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00313

The client MUST include a Replace for the ./DevInfo/Ext/RCSEnabled in all MsgID 1 messages to the server. The content of this node must be the current user enablement setting for RCS. If the user has enabled the service, the value for this node must be '1'. If the user has disabled the service, the value for this node must be '0'.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00316

User Equipment MUST fall back to another access technology when the OMA DM session is unable to be established. Example. ("When connected to Wifi if an OMA DM session is unable to reach the requested IP address the UE MUST connect to the next available cellular connection and attempt the connection again.")

Priority: Must

Category: Cat1

Device: Smartphone

2.2.1 Airplane Mode Requirements

The Airplane Mode is an off condition for the radio, so the device is unable to receive NIA messages. The device is also unable to initiate OMA-DM sessions.

OMA-SIMOTA-00040

The device must never initiate an OMA-DM session while in Airplane Mode. This includes all client-initiated sessions and network-initiated sessions.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00041

The device must queue a NIA received immediately prior to entering Airplane Mode and respond to it when exiting Airplane Mode.

Priority: Must

Category: Cat1

Device: Smartphone

2.3 User-Agent String

A user-agent header in the HTTP messages will facilitate troubleshooting. This header must be available when logging at the various network elements and must accompany each message, without affecting the content of the synchml messages.

OMA-SIMOTA-00042

The client must add a User-Agent header to all HTTP messages during a management session.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00043

The User-Agent header must be in the following format:

User-Agent: <make>/<model>/<Device ID>/<DM-vendor>/<DM-version>

Where <make> is the manufacturer and

<model> is the model name

<Device ID> is the IMEI or MEID of the device whichever is being used as the dev_id

<DM-vendor> is the OMA-DM client vendor and

<DM-version> is the version of the OMA-DM client.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00044

Each token must NOT contain spaces. Underscore (‘_’) characters and dashes (‘-‘) are permitted. Do NOT use the ‘<’ or ‘>’ symbols in the string. Spaces are only allowed as defined in the format described above.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00045

The allowed character set within each token is US-ASCII 0x21 through 0x7E, inclusive.

Priority: Must

Category: Cat1

Device: Smartphone

3 Network Initiated Details

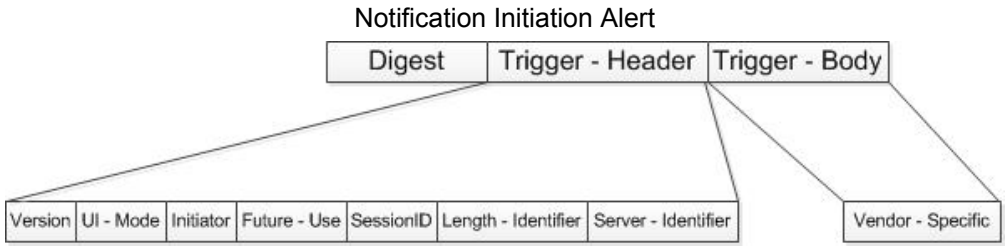
Sprint Nextel provides activation, customization, customer-care functionality and miscellaneous services that utilize server-initiated OMA-DM sessions.

Management sessions with the device can be initiated by the OMA-DM server using the Notification Initiation Alert described by the OMA in [DM Notification]. The Notification Initiation Alert will be carried in the payload of a WAP-encoded SMS message. The format of this WAP Push and expected device behavior is described in the sections below.

The payload of the Notification Initiation Alert ("NIA") message is shown below.

A full description of each field is contained in Section 6 of [DM Notification].

In general, the message payload mostly comprises a server account identification pointing to a server account preconfigured in a DM tree node. The DM application will initiate a DM session with the specified server indicating to it that the session was initiated because of network initiation.



3.1 Notification Initiation Alert (NIA) - Handling

OMA-SIMOTA-00046

The device must support receipt of the Notification Initiation Alert message (Package 0).

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00047

The server will support multiple "commands" per DM Session. The device must support the execution of multiple management commands in a single management session.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00048

The device shall support the receipt and handling of multiple (erroneous/duplicate/retry) NIA messages. If the device has already received an NIA from the server and receives a new one with the same session ID, it must replace the existing NIA with the new one.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00049

If the device receives another NIA with a different session ID, the device shall respond to both messages in a first-in first-out (FIFO) order.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00050

The DM client shall store the NIA until it can be executed. The device must execute the NIA immediately when there is not a voice call in progress.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00051

The DM client must execute immediately, even if there are background processes running. The device must NOT be required to be on a home screen to process the NIA.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00052

The device must execute an NIA while on home or roaming networks unless the user has selected to turn data roaming off.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00053

The NIA message shall be hidden from the user. Do not display the contents of the NIA to the user.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00054

The user shall not have the ability to view or manage the NIA.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00055

After executing the DM Session, the device must delete the NIA from its queue.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00034

During network-initiated transactions, if the DM Client fails to connect to the server it must retry up to 25 hours after receiving the NIA. The DM Client must confirm whether data network is available or not at 5minutes, 10minutes, 20minutes, 40minutes, 60minutes, and then keep retrying every 60 minutes after receiving the NIA. If the DM Client retries the maximum amount of time has passed, the DM Client must delete the NIA. These retrys must NOT happen while the device is in airplane mode.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00056

The device must execute the NIA when in a locked mode, such as Restrict And Lock, an OEM specific lock mode, or an OS specific lock mode.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00035

During network-initiated transactions if the client connects to the server but receives a well-formed package 2 from the server containing an error, the client must NOT retry and must delete the NIA.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00281

The device must ignore the first 4 bytes of the WAP message received from Sprint's OMA DM server.

Priority: Must

Category: Cat1

Device: Smartphone

3.2 Network Initiated UI Flow

OMA-SIMOTA-00057

When the device is locked, the NIA must be executed in the background. The NI must be automatically canceled by the client if the user taps the emergency call button or makes a 911 call.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00058

All devices must conform to the verbiage and functionality of the user interface requirements described in this document. This includes connection manager software running on a PC, admin consoles for mobile broadband products, traditional handsets, smartphones, and all other device types.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00059

Device vendors are permitted to implement the user interface requirements into their respective themes, but are NOT permitted to change the verbiage or functionality such as cancel buttons and behaviors.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00060

The UI Mode will determine how the UI screen will be displayed.

Pkg 0 UI Mode Transaction Matrix		
UI_MODE (bits)	**Decimal**	**Name**
00	0	NOT_SPECIFIED
01	1	BACKGROUND
10	2	INFORMATIVE
11	3	INTERACTIVE

Table 2 - UI Mode Definition

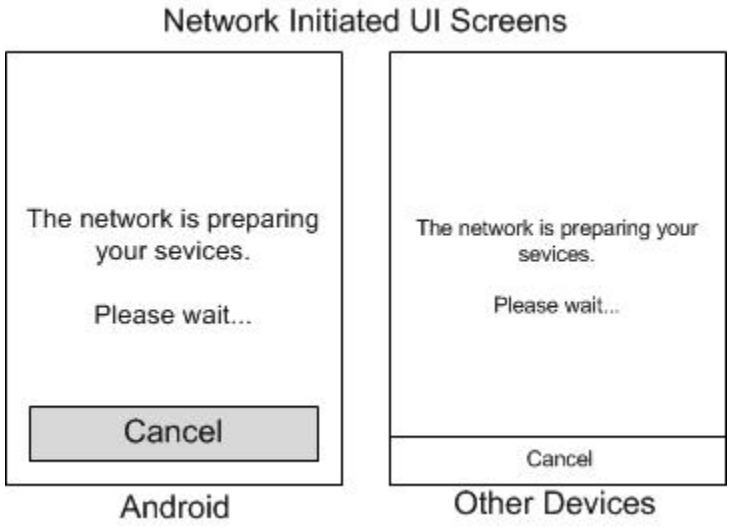
Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00061

The device must display the following UI screen for all management sessions initiated from the network with a UI_MODE of NOT_SPECIFIED, INTERACTIVE or INFORMATIVE:



Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00062

For BACKGROUND network initiation alerts, the device must not display the Network Initiated UI Screen from DM-UI-05 unless the user presses a key, makes a gesture on the touchscreen or opens the flip/slide.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00063

The DM client must not display any errors during a BACKGROUND session unless the Network Initiated UI Screen from OMA-SIMOTA-00061 is currently displayed. If the screen is not displayed, there must not be any error message displayed to the user for that session.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00064

If the device receives an NIA with UI_MODE set to INTERACTIVE, the DM client must behave as though the UI_MODE was set to INFORMATIVE

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00065

The device must not implement screens that differ from those defined within this document. The NIA does not contain enough information to know why it was sent. Therefore, the DM client cannot use screens that are specific to any NIA received.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00066

The network initiated UI requirements defined in this section MUST apply to every NIA sent, for any purpose. All NI-transactions will use the same UI requirements.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00067

The device shall allow the user to cancel the NI- session by pressing the "Cancel" button, "END" key or the [RSK] as defined in the Network Initiated UI Screen from OMA-SIMOTA-00061.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00068

Connection manager software and touchscreen devices must implement a cancel button in the dialog displayed to the user.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00069

When the NI transaction has been successfully completed, the device shall return to the home/standby screen. On some devices it is permitted to return to the previous context instead of the home/standby screen (eg Android, Windows, connection managers, etc.).

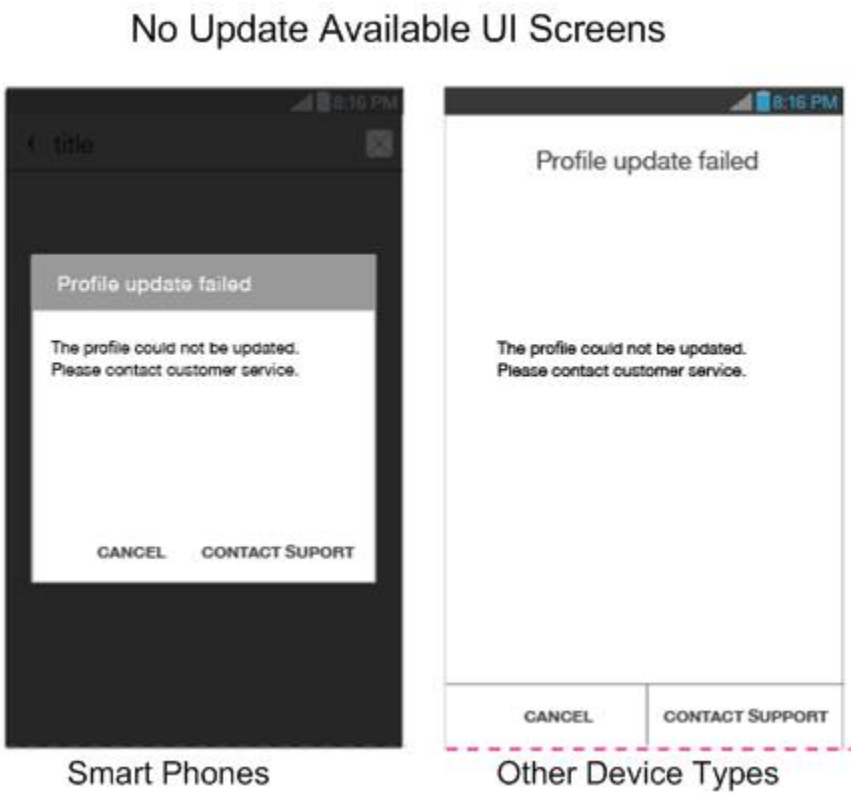
Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00070

If the server does not provide any provisioning information, the device must display the following UI screen. This is a narrow edge case that is unlikely to happen, but if the server does not return profile information the device must display feedback to the user.



Priority: Must

Category: Cat1

Device: Smartphone

4 Client Initiated Details

Device management sessions can also be initiated from the device. In general, the initiation of such sessions is triggered by a user's action, but they can also be triggered by some other event.

OMA-SIMOTA-00071

The device must allow client-initiated sessions to be initiated. For example, mobile broadband products must implement them in an admin console, smart phones and traditional handsets must have menus to trigger them, modules or embedded products must use AT commands, etc.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00072

The device must allow client-initiated transactions to be triggered automatically after a firmware update. Scenarios for this include ~~FUMO looping during HFA and~~ performing a CIDC after a proprietary FOTA upgrade.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00073

The device must allow client-initiated transactions to be triggered after installing applications.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00074

The device must allow client-initiated transactions to be triggered after Exec operations.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00075

The device must allow client-initiated transactions to be triggered by other applications via an API exposed by the OMA-DM client.

Priority: Must

Category: Cat1

Device: Smartphone

4.1 Client Initiated Device Configuration Alert Codes

OMA-SIMOTA-00076

The following table contains the alert 1226 type codes to be used for CI Provisioning Requests

Alert 1226 Type Codes			
Client Initiated Provisioning Request	SIM OTA Devices	HFA	org.openmobilealliance.dm.simotaconfiguration.hfa
		User Initiated	org.openmobilealliance.dm.simotaconfiguration.userrequest
		Device Initiated	org.openmobilealliance.dm.simotaconfiguration.devicerequest

Table 3: Alert 1226 Codes for CIDC

Priority: Must

Category: Cat1

Device: Smartphone

4.3 Client Initiated FUMO Alert Codes

OMA-SIMOTA-00077

The following table contains the alert 1226 type codes to be used for CI FUMO Requests

Alert 1226 Type Codes			
Client Initiated FUMO Request	HFA	CDMA, CSIM and eCSFB	org.openmobilealliance.dm.firmwareupdate.devicerequest
	User/Device Initiated		org.openmobilealliance.dm.firmwareupdate.userrequest

Table 5: Alert 1226 Codes for CI FUMO

Priority: Deprecated

Category: Cat1

Device: Smartphone

4.4 Client Initiated UICC Unlock Alert Code

OMA-SIMOTA-00078

The following table contains the alert 1226 type codes to be used for CI UICC Unlock Requests.

Alert 1226 Type Codes			
Client Initiated UICC Unlock Request	User Initiated	CDMA, CSIM and eCSFB	org.openmobilealliance.dm.encryptunlocksim.userrequest

Table 6: Alert 1226 Codes for UICC Unlock

Priority: Must

Category: Cat1

Device: Smartphone

5 Device Configuration

Device Configuration is defined as the programming of the necessary parameters to access network voice and/or data services. This transaction is used to activate new devices, reactivate devices on a new account, modify the parameters for an existing subscription and customize the device.

OMA-SIMOTA-00079

The DM client must support activation, modification and reactivation of a device using any set of nodes from the [Sprint DDF]. The nodes will not be in any particular order and the collection of nodes in the management session will not be consistent.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00080

The OMA-DM Client shall timeout any HTTP connection that does not receive a response in 60 seconds. The management session may take longer to complete, however the client should only timeout when there is more than 60 seconds between packets.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00081

The OMA DM client must overwrite the entire length of any object with the value provided in the management command. This applies to EVERY node in the [Sprint DDF].

Example: When the NAI changes, the entire length of the NAI must be overwritten with the new value.
Previous value: OMADMTEST@sprintpcs.com
New value: OMA@sprintpcs.com
Incorrect! OMA@sprintpcs.comcs.com

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00084

The device is not required to reboot if settings change unless it is needed to successfully apply the updates.

Priority: Must

Category: Cat1

Device: Smartphone

5.1 Client Initiated Device Configuration (CIDC)

OMA-SIMOTA-00085

The user shall have the ability to manually initiate a device configuration session with the server. See the **Client Initiation Details** section for more information.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00086

The OMA-DM Client shall conduct the session with the server as defined in [OMA-DM Session Details] section.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00087

The device shall allow other applications to initiate a CIDC session if slot-1 is not programmed.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00088

The DM client must execute the device configuration session in accordance with standard protocol messaging defined in [DM RepPro].

Priority: Must

Category: Cat1

Device: Smartphone

5.2 Client Initiated Device Configuration UI Flow

OMA-SIMOTA-00091

During a CIDC session the UI screen in GTR-UICC_TERMINAL-00166 shall be displayed to the user.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00092

The user shall have the ability to cancel a CIDC session by pressing the [RSK] or cancel button in the dialog.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00093

The device shall return to the home/standby screen when the CIDC session is successful. This only applies to instances when the session was started by the user. Multi-process devices such as Android, Windows, RIM, etc. are permitted to return to the calling context instead of a home screen.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00094

The device shall return to the calling application (Wireless Backup, Browser, etc) after successful completion of the CIDC.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00095

If a CIDC session is started by the user and no profile information is available on the server, the device must display the UI screen in GTR-UICC_TERMINAL-00168. This screen is only displayed when the client successfully connects to the server without error and receives an empty session.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00096

The device must allow a Client Initiated Device Configuration (“CIDC”) session to be triggered from an “Update Profile” menu/button defined in:

GTR-UICC_TERMINAL-00164

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00279

If a CIDC session completes successfully, the UI screen in GTR-UICC-00173 must be displayed.

Priority: Must

Category: Cat1

Device: Smartphone

6 Hands Free Activation

Hands-Free Activation (“HFA”) is a series of client-initiated commands to be performed on power-up of a new or reset device. This set of commands provides a streamlined mechanism for ensuring that a device is updated with the latest settings during the time of activation. This process flow is designed to be very simple and easy for the user to understand. It is designed to allow the user to cancel at any time.

OMA-SIMOTA-00097

The device MUST complete ~~each step of~~ the HFA process. If ~~each step is not completed, the device MUST re-attempt that step on the next power up. For example, if~~ the CIDC~~FUMO portion of HFA~~ fails, the device must perform a CIDC~~FUMO~~ on the next power up. ~~For FUMO, no update found does not count as a failure. A device that does not use Sprint's FUMO for firmware updates and includes a Replace for the ./DevDetail/SwV in all MsgID 1 messages to the server does not need to support the CIFUMO request during HFA.~~

Priority: Must

Category: Cat1

Device: Smartphone

6.1 Hands Free Activation Conditions

OMA-SIMOTA-00098

A user must be able to cancel any HFA session by holding the "Back" key for 5 seconds.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00099

HFA must be triggered on next power-up after being reset or refurbished (e.g. ##RTN#, ##SCRTN#. ##BRAND# or an over-the-wire tool) if Mobile Data is enabled.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00100

A device that supports Wifi, must perform HFA over Wifi if it is connected to Wifi when the HFA conditions in are true.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00101

A device that supports LTE, must perform HFA over LTE if it is able to attach on the OTA APN when the HFA conditions are true.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00102

The HFA sequence of commands must be in the following order:

First, CIDC as defined in the [Device Configuration] section.

- Up to five (5) retries as defined in this section

~~Second, CIFUMO as defined in the [OTA Firmware Updates] section but using the CIFUMO (HFA) alert string defined in [Table 3 - Alert 1226 Type Codes].~~

~~- CIFUMO loop until no more updates are found~~

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00103

The CIFUMO loop of transactions during HFA must only occur if the CIDC was successful. The CIDC is successful if the device receives a payload from the server, even if it is the same already in the device. The CIFUMO during HFA will run immediately after the CIDC completes.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00104

The CIFUMO during HFA must repeat until it finds no more updates available, defined by the empty management session. If there are two firmware updates available, the device will loop through two complete CIFUMO updates. Here is the sequence in this example:
Power up -> CIDC -> CIFUMO -> User opt-in -> install -> reboot -> CIFUMO -> User opt-in -> install -> reboot -> home/idle.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00105

The 1226 alert code strings for HFA are listed in Client Initiated section.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00106

The HFA transaction cannot be canceled by closing the flip, sliding the device open or closed, or by any button except for the Cancel button, emergency call button, RSK or the [END] key.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00107

If the HFA management session successfully completes, the device shall reboot if necessary and go to the home/ idle screen.

Note, it is permissible for the device to automatically reset or reboot after a successful HFA.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00108

If the device encounters an error, the device shall display the error code and description then stop. The device shall NOT retry if an error occurs. “Errors” are defined as MIP errors, proxy errors, HTTP errors or other well-formed OMA-DM protocol errors, except 407 and 404. Encountering an error is different from “no profile” described below.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00109

If the device connects to the OMA-DM server and no profile information is available, the device shall perform retries as described below. The device shall only retry when successfully connecting to the server and no profile information is available as defined by a well-formed 407 protocol error received in package 2.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00110

The number of retries performed during the CIDC transaction in the HFA sequence must be set to 5.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00111

The retry interval during the CIDC transaction in the HFA sequence must be set to 60 seconds.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00113

If the user cancels or aborts the transaction, the device shall not attempt another HFA until the device is power cycled and the conditions for HFA are met.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00114

If the user cancels or aborts before all the retries are completed, the device shall not attempt another HFA until power cycled. Also, if an error occurs the device shall stop the HFA and not attempt again until next power cycle.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00115

If a user resets or refurbishes the device with a ## command, PST tool or other OEM-specific tool, the device must attempt HFA on power up as described in [Fig. 6 – HFA Flow].

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00117

If Mobile Data has been disabled, the client MUST NOT start HFA, even if the conditions have been met.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00118

HFA MUST be allowed to take place prior to any Anti-Theft User Authentication on the device.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00120

The OMA DM client must not request a reboot following HFA completing unless it is able to read the MSISDN (EFID 6F40) and validate that it is not in the factory default state of FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00121

If the OMA DM client has completed all steps of HFA and the MSISDN (EFID 6F40) is still the factory default value of FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF ~~000000xxxx~~, the client must wait 2 seconds and then read it again.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00122

If, after 30 seconds, the MSISDN (EFID 6F40) is still in the factory default state of FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF, then the OMA DM client must request a reboot if needed and continue with OOBE.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00142

If the device does not support FUMO using Sprint's OMA DM server and includes a Replace for the ./DevDetail/SwV in all MsgID 1 messages to the server it does not need to perform a CI FUMO request during HFA.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00314

If a new Sprint SIM is inserted into the device, the OMA client must perform a CIDC.

Priority: Must

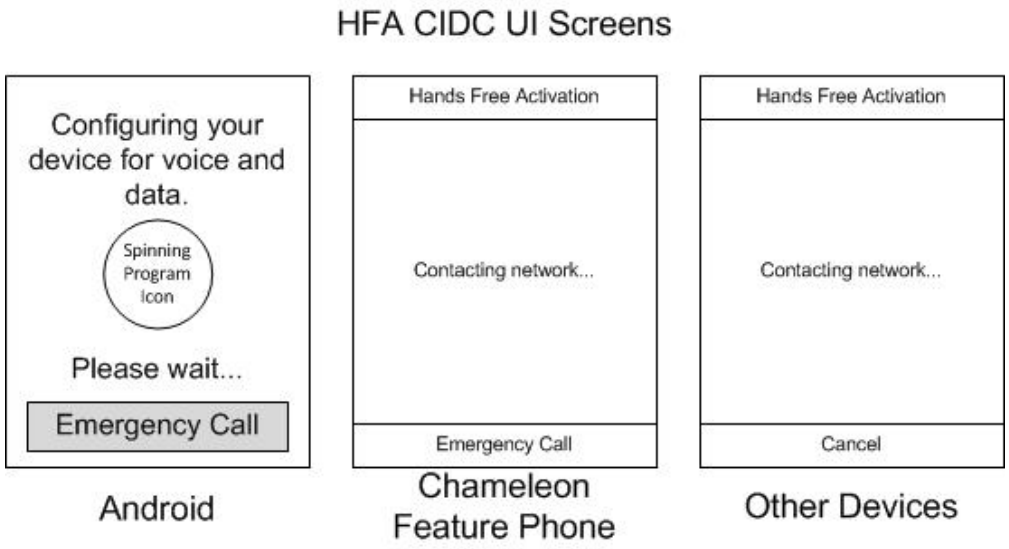
Category: Cat1

Device: Smartphone

6.2 Hands Free Activation UI Flow

OMA-SIMOTA-00124

The HFA CIDC UI screen should be as follows:



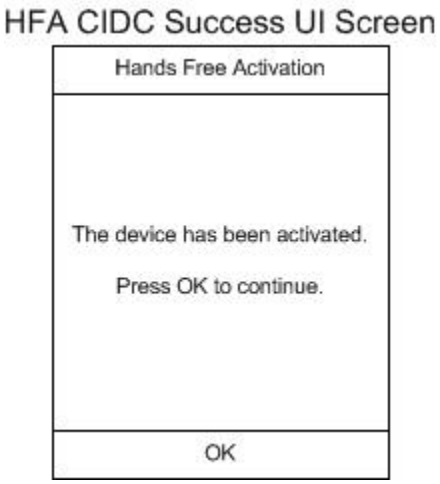
Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00125

If the HFA CIDC is successful, the following UI screen must be displayed for a non-Android device.



Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00127

If the CIDC portion of HFA is successful, the device must ~~begin the CIFUMO portion of HFA~~ continue OOBE when the "OK" button/[RSK] is pressed or after 5 seconds have passed.

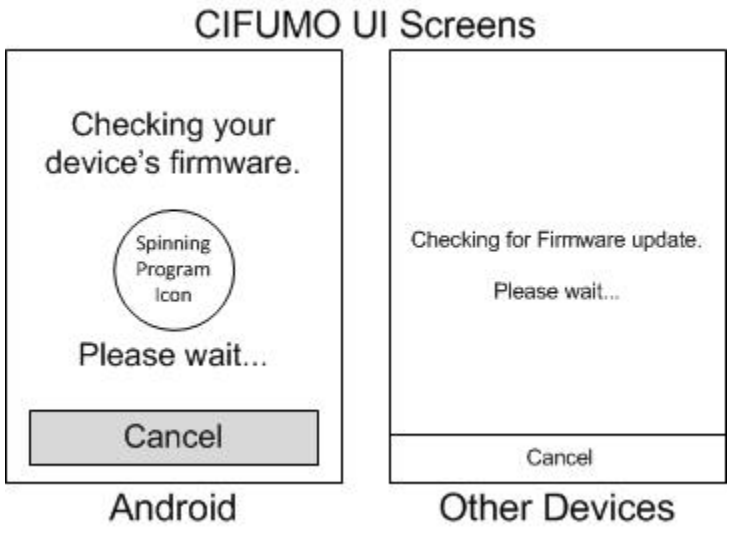
Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00128

The HFA CIFUMO UI screen should be as follows:



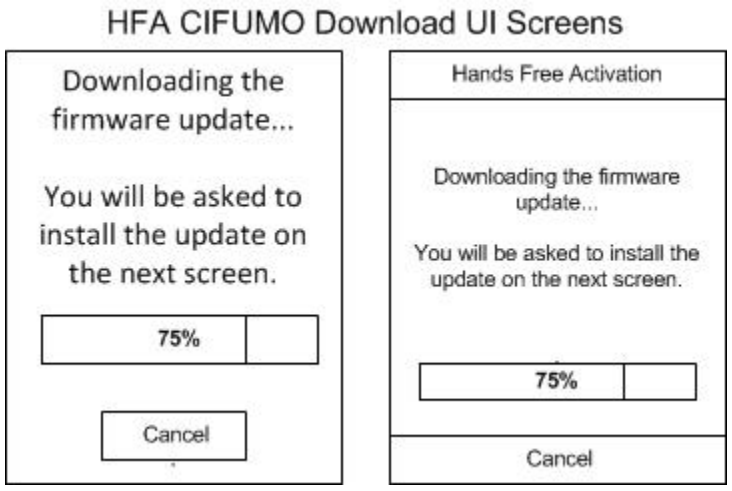
Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00129

If the server returns a URL and exec command UI Screen 12: HFA FUMO DL must be displayed.



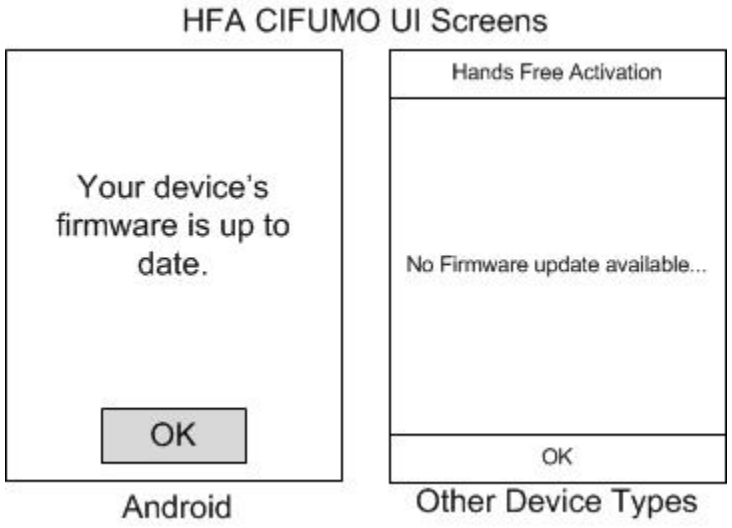
Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00130

If no FUMO update is available, the device must display the following UI screen.



Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00132

If the Emergency Call button is tapped or the Right soft key is pressed, the device must stop the OMA session and launch the emergency dialer.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00133

If an emergency call was made, the device must not go back to the previous UI Screens until Emergency Mode has ended either by user interaction or by timer expiration.

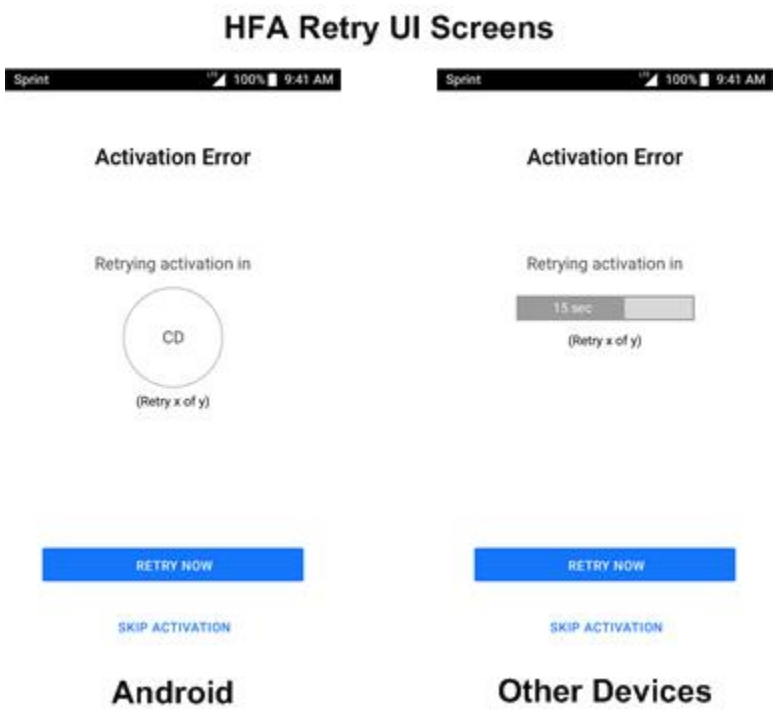
Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00134

If the server returns a well formed 407 after the HFA CIDC request, the following UI screen must be displayed.



Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00135

The device must display a progress bar or other time indicator to the user during the 60 second retry interval. Also, the device must show the number of retries left.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00136

When the 60 second timer expires and the device begins a retry, it shall display the HFA UI screen described in DM-UI-15.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00137

The [Retry] key (LSK) must immediately relaunch the CIDC transaction.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00138

If the user presses the Cancel (RSK) or [END] button, the device shall stop any OMA-DM session and go to the home/idle screen.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00139

If the Emergency Call button is tapped or the Right soft key is pressed, the device must launch the emergency dialer.

Priority: Should

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00140

Once the emergency dialer is exited, the device must return to the UI screen that it was launched from and restart the OMA session.

Priority: Should

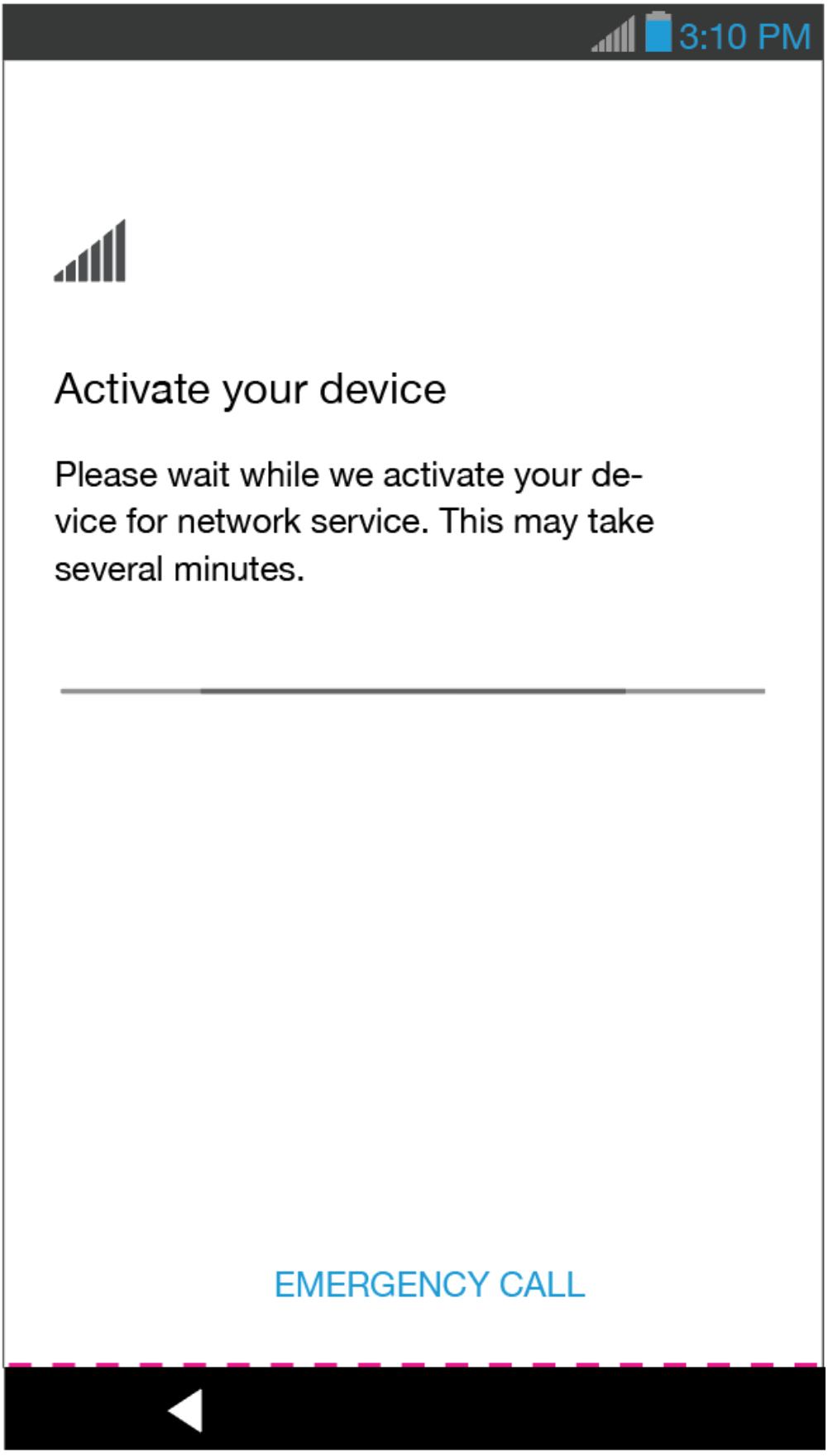
Category: Cat1

Device: Smartphone

6.3 HFA for Smart Phones and Tablets

OMA-SIMOTA-00141

The following UI screen must be used for all OMA HFA sessions including the first HFA retry countdown. This UI screen MUST follow the WiFi setup screen.


3:10 PM
Activate your device
Please wait while we activate your device for network service. This may take several minutes.
EMERGENCY CALL

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00143

If the settings delivered by the OMA server can be applied with just a radio reset, and the client is able to read an MSISDN from the UICC that is not in factory default format, the device must proceed to the OMA-Complete UI screen as displayed in the Setup Wizard / Mobile ID GTR.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00144

If the settings delivered by the OMA server cannot be applied with just a radio reset and the client is able to read the MSISDN from the UICC and it is not in factory default format, the device must reboot and then proceed to the OMA-Complete UI screen as displayed in the Setup Wizard / Mobile ID GTR.

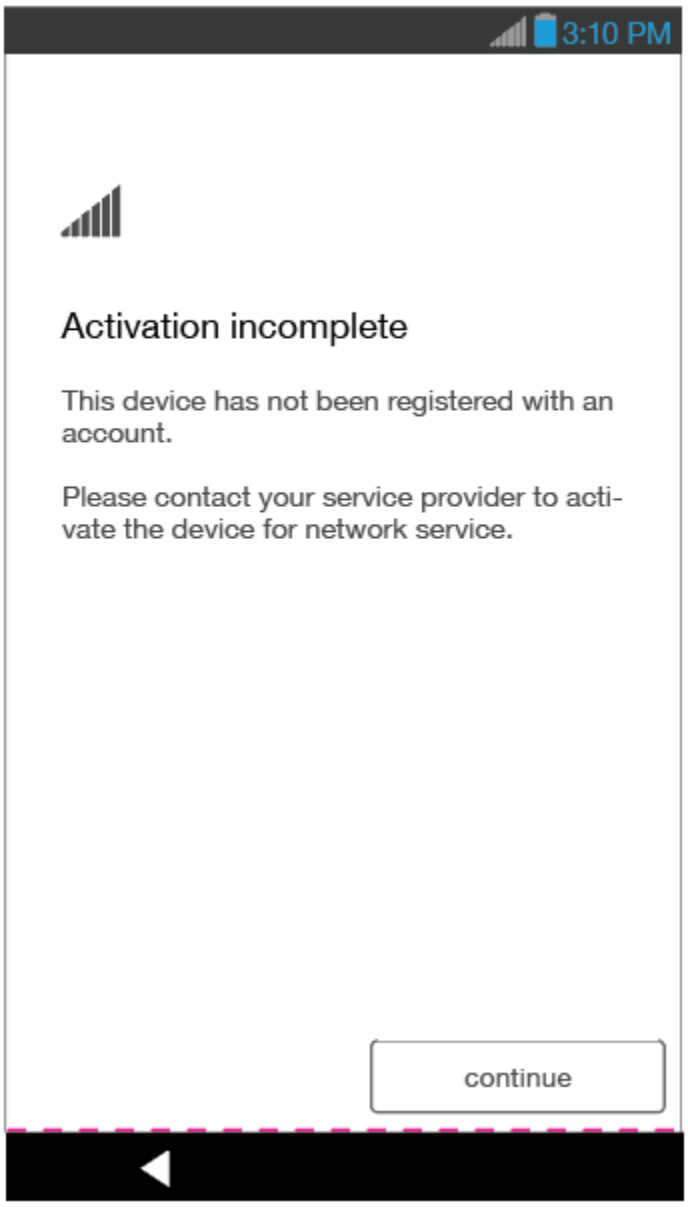
Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00145

If a network error occurs, the error message must be displayed to the user in the lower left hand corner of the following UI screen above the Continue button. If the user hits the continue button, the device should continue to the setup wizard.



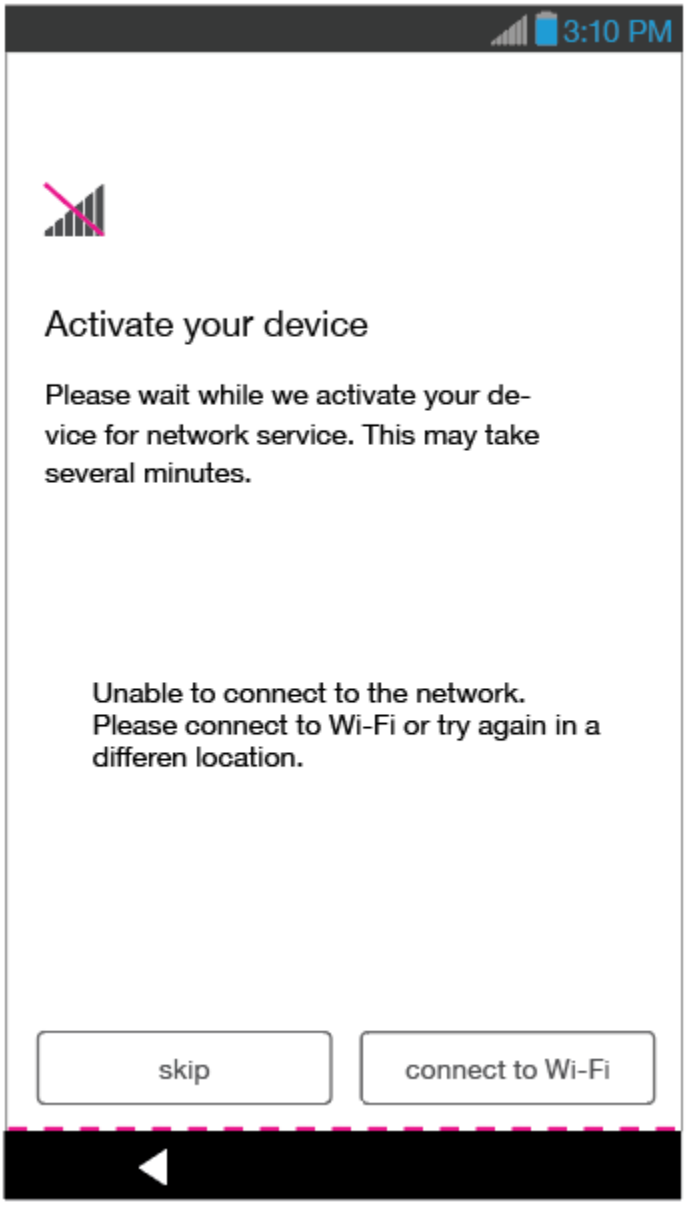
Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00304

If the OMA Client is not able to reach the OMA DM server over LTE, eHRPD, HRPD or 1xRTT, the following UI Screen must be displayed. If the user selects 'skip' the device must continue OOBE. If the user selects 'connect to Wi-Fi', the device must go back to Wi-Fi setup. If the user sets up a Wi-Fi connection the device must launch HFA from the beginning.



Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00146

If the client receives a connection timeout for the CIDC session, the client must stop HFA and continue into Setup Wizard. Every 2 hours, the client must launch the CIDC portion of HFA again in the background until the session completes. The must be a notification in the notification bar showing the status of the time till next attempt that will also allow the user to initiate an immediate attempt.

Priority: Must

Category: Cat1

Device: Smartphone

6.3.1 SMF Validate Device

OMA-SIMOTA-00147

If the OMA client receives a well formed 407 from the OMA server during the first CIDC session of HFA, it must call the SMF client according to requirement SMF-00044 in the Sprint Mobile Framework specification. The client MUST keep displaying the UI screen in OMA-SIMOTA-00141 until it receives a response from SMF.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00148

If SMF returns a "VALIDATION_STATUS_ALREADY_ACTIVE" status or an exception, the OMA client must perform HFA Retries.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00149

If the SMF client returns a "VALIDATION_STATUS_AVAILABLE", "VALIDATION_STATUS_UICC_ACTIVE" or "VALIDATION_STATUS_UICC_AVAILABLE" status, the OMA client must launch the SMF UI following requirement SMF-00045 in the Sprint Mobile Framework specification.

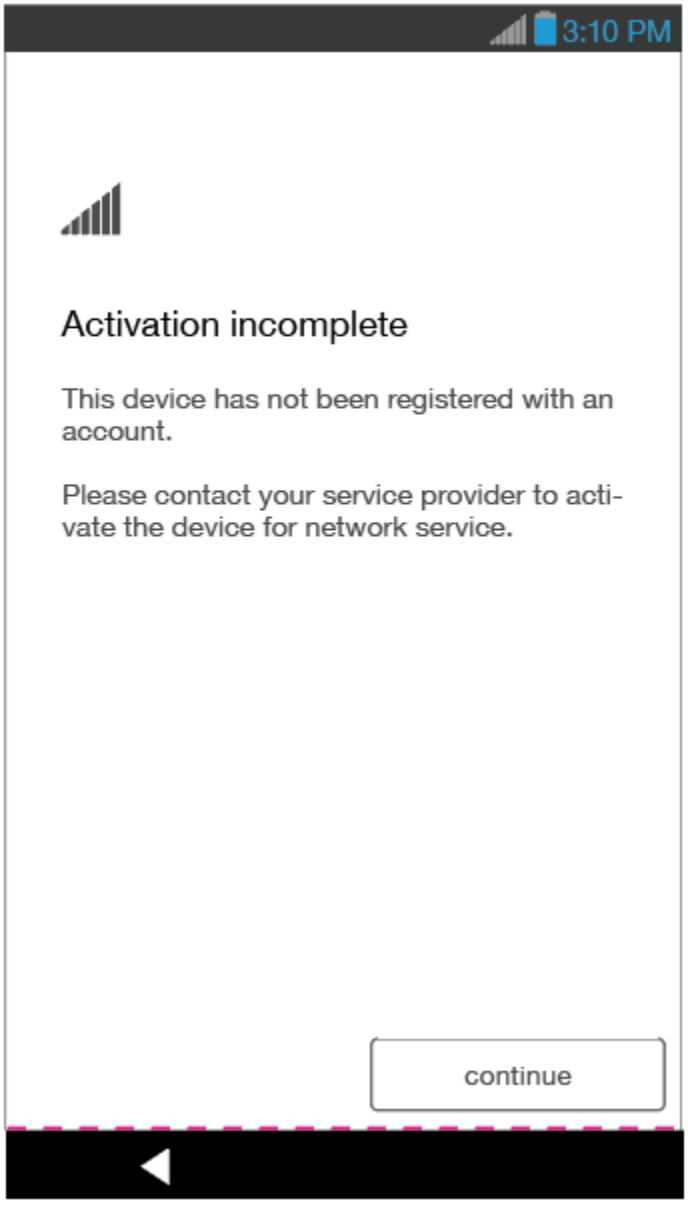
Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00150

If SMF returns any other status than "VALIDATION_STATUS_ALREADY_ACTIVE", "VALIDATION_STATUS_AVAILABLE", "VALIDATION_STATUS_UICC_ACTIVE" or "VALIDATION_STATUS_UICC_AVAILABLE" the client must display the following UI screen.



Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00151

If the user taps continue, the device must continue into the setup wizard.

Priority: Must

Category: Cat1

Device: Smartphone

6.3.2 SMF Start Activation Process

OMA-SIMOTA-00152

If SMF returns a status of STATUS_ACTIVATED, the client must start HFA over from the beginning.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00153

If SMF returns a status of STATUS_SKIPPED, the OMA client must send the user to the Wifi setup UI Screen in the Setup Wizard.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00154

If SMF returns a status of STATUS_FAILED, the device must go to the Wifi setup UI screen in Setup Wizard.

Priority: Must

Category: Cat1

Device: Smartphone

6.3.3 HFA Retries

OMA-SIMOTA-00155

The retry interval during the CIDC transaction in the HFA sequence must be set to 40 seconds.

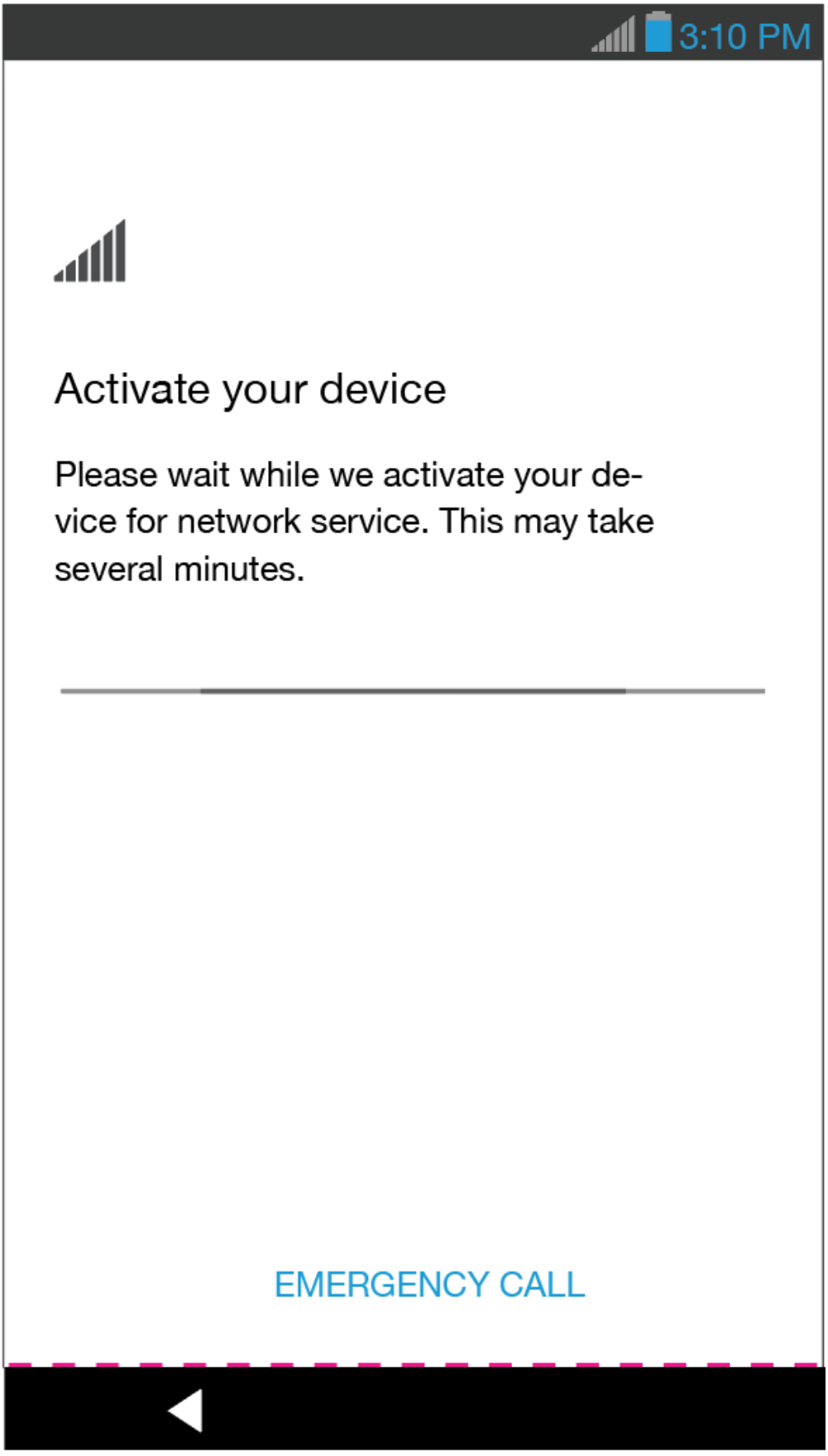
Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00156

For the first HFA Retry, the following UI Screen must be displayed.


3:10 PM
Activate your device
Please wait while we activate your device for network service. This may take several minutes.
EMERGENCY CALL

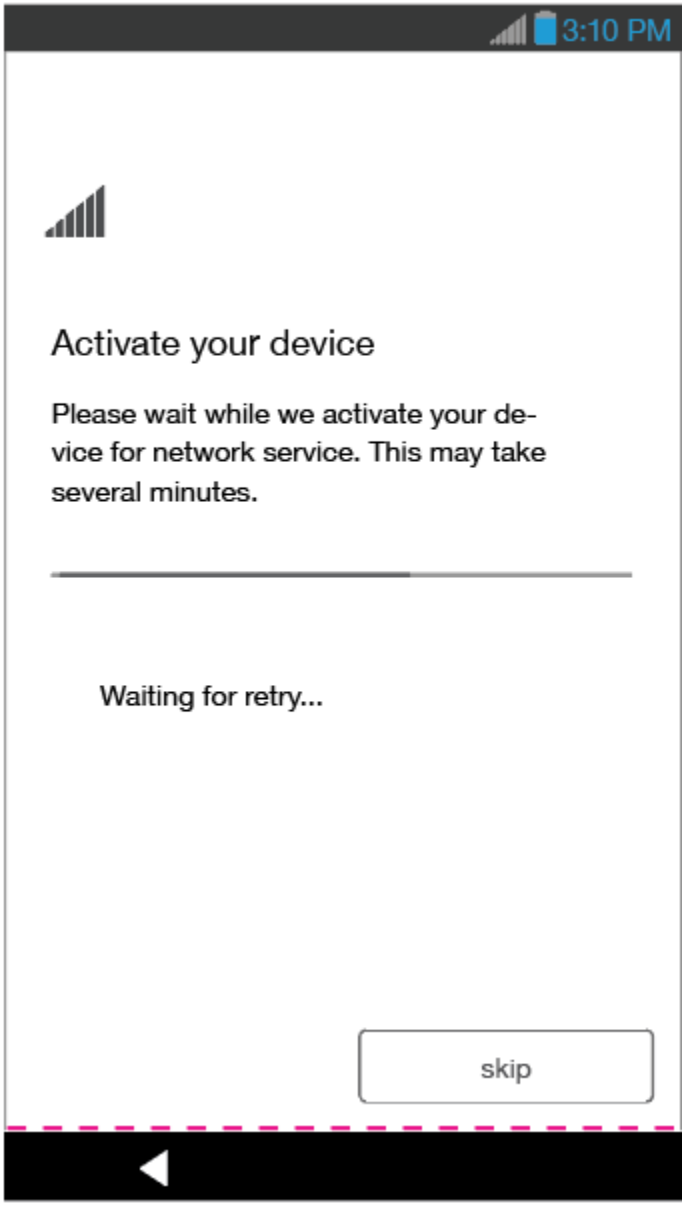
Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00157

The following UI screen must be displayed if the client receives a well formed 407 from the OMA server in response to the first retry attempt.



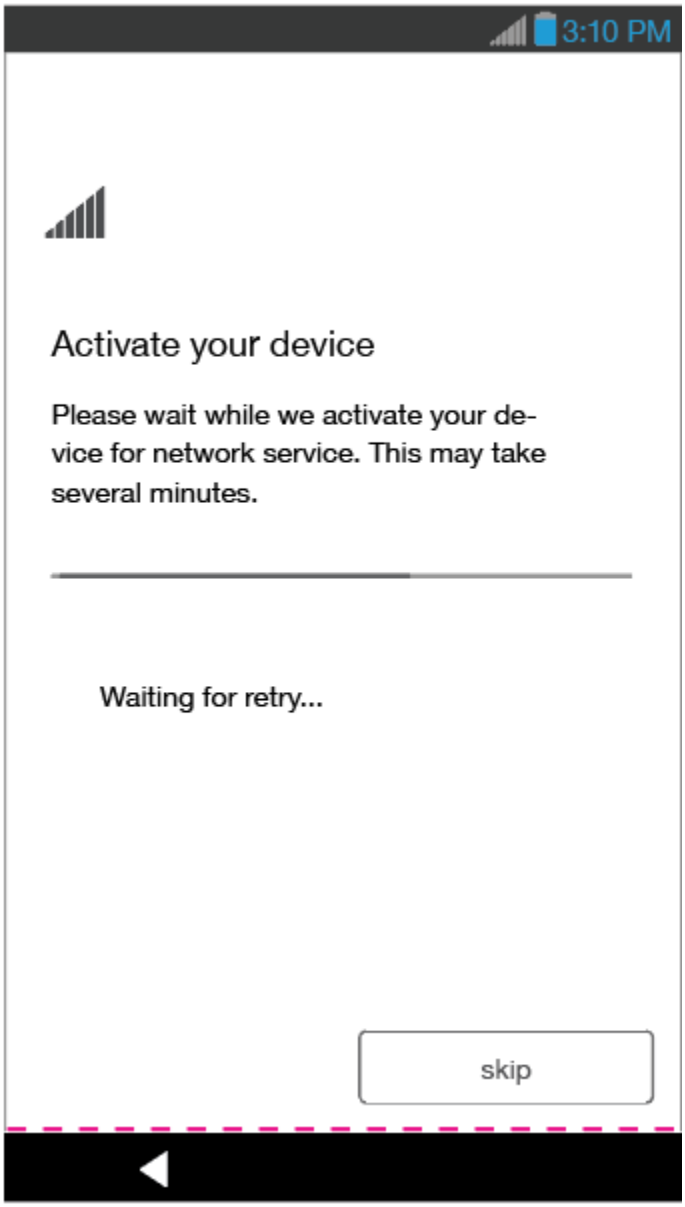
Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00158

If the OMA client receives a well formed 407 from the OMA DM server after the second retry attempt, the following UI screen must be displayed.



Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00159

If the user taps Skip, the device must continue the Setup Wizard.

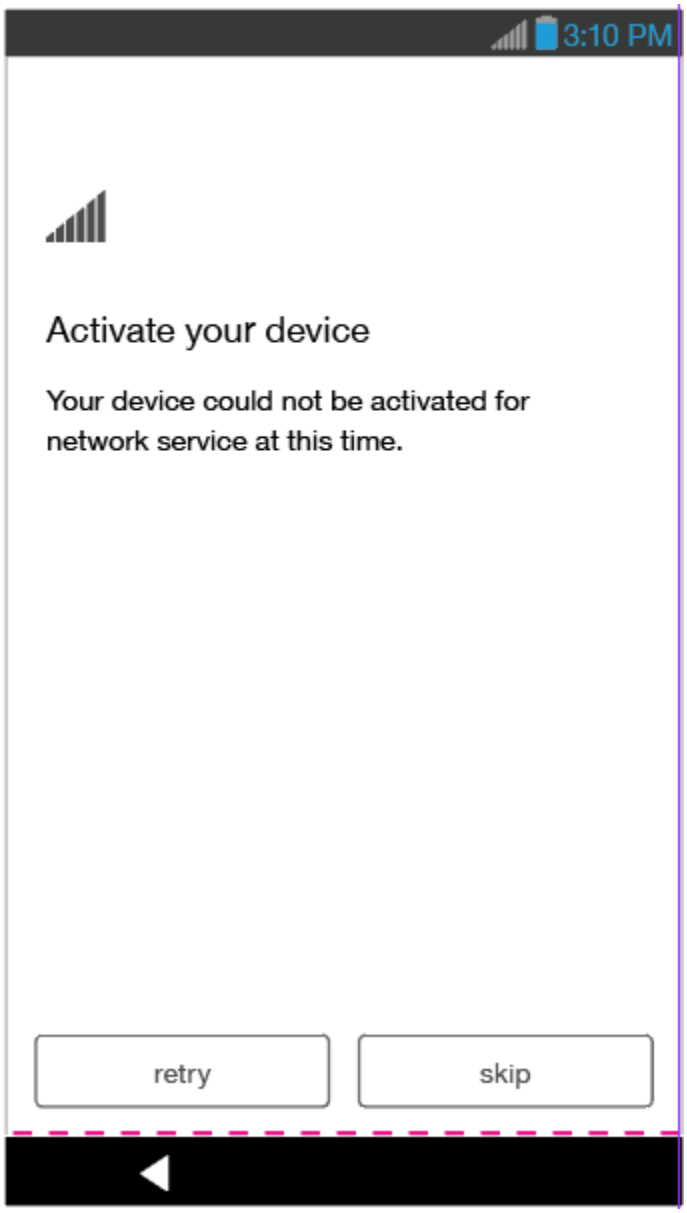
Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00160

If the OMA client receives a well formed 407 after the third retry attempt, the following UI screen must be displayed.



Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00161

If the user selects the Retry option, the client must start HFA Retry's again and display the UI screen in OMA-SIMOTA-00157.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00278

During the interval between HFA Retry attempts, the screen must display a countdown until the next Retry attempt.

Priority: Must

Category: Cat1

Device: Smartphone

7 OTA Firmware Updates

Sprint requires that all devices support an OTA firmware update mechanism. If an OEM has their own FOTA platform then they must support the Alternative Firmware OTA requirements as well as performing a CIDC~~FUMO~~ request to Sprint's OMA DM server during HFA as well as after an Alternative Firmware update. ~~If an OEM is using a third party OTA update firmware update mechanism, then they must fully support Sprint's FUMO requirements as well.~~

OMA-SIMOTA-00315

The device must ~~support a method to~~ initiate a CIDC to Sprint's OMA DM server following a successful FOTA update.

~~This must only be used as requested by Sprint for an MR.~~

Priority: Must

Category: Cat1

Device: Smartphone

7.1 Firmware Update Management Object

OMA-SIMOTA-00167

The device support firmware updates using the FUMO 1.0 standard management object.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00168

The device must support Firmware Updates using Alternative Download (OMA-DL), in compliance with OMA-DL 1.0 [DL OTA].

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00169

The ./FWUpdate/Flash/Download/PkgURL and ./FWUpdate/Flash/DownloadAndUpdate/PkgURL nodes are executable nodes that trigger the invocation of the firmware update process. Since this process is OEM-specific, the mechanism will be implemented specifically by each OEM.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00170

The device OEM should use a diff technology to generate the smallest packages possible. It recommended that installations not exceed 10 minutes, not including the time required to download the software.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00171

After the final status of a successful installation, the DM client must perform another CIFUMO until no more updates are available. This applies to installations that occurred as a result of either CIFUMO and NIFUMO.

Priority: Deprecated

Category: Cat1

Device: Smartphone

7.2 Client Initiated Firmware Update (CI-FUMO)

OMA-SIMOTA-00172

When a user initiates a new firmware update, the device shall check the reserved firmware package memory space for the presence of a download descriptor and binary package.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00173

If one or both (binary package or download descriptor) are missing, the device must delete them and execute a new CIFUMO transaction.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00174

The DM Client shall use the CI FUMO generic alert defined in [Table 5: Alert 1226 Codes for CI FUMO].

Priority: Deprecated

Category: Cat1

Device: Smartphone

7.3 Network Initiated Firmware Update (NI FUMO)

Sprint will trigger network-initiated firmware updates using the NIA described in the [Network Initiation Mechanism] section.

OMA-SIMOTA-00175

The download of an available update MUST begin automatically. The device MUST NOT prompt the user to begin the download.

Priority: Deprecated

Category: Cat1

Device: Smartphone

7.3.1 Download Descriptor Format

OMA-SIMOTA-00176

The device must support the Download Descriptor format defined in the [DL OTA] standard.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00177

The <installParam> element will contain the estimatedInstallTimeInSecs value.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00178

The <size> element must be used as the max value when displaying the progress bar during the download.
Here is an example of the download descriptor (INFORMATIVE only):

```
<?xml version="1.0" encoding="UTF-8" ?>
<media xmlns="http://www.openmobilealliance.org/xmlns/dd">
<DDversion>1.0</DDversion>
<name>testdelta1</name>
<type>application/octet-stream</type>
<description>Firmware update description that can be 1,500 characters long</description>
<objectURI>http://tdas3035.test.sprint.com/agents/200012/1/testdelta1.bin </objectURI>
<size>5061</size>
<installNotifyURI>http://tdas3035.test.sprint.com/omadl/
status?h=69643D32393226723D313331373633</installNotifyURI>
<installParam>estimatedDownloadTimeInSecs=1234&estimatedInstallTimeInSecs=567</installParam>
<vendor>SPRINT_NEXTEL</vendor>
</media>
```

Priority: Deprecated

Category: Cat1

Device: Smartphone

7.4 FUMO UI Screens

OMA-SIMOTA-00196

Android devices must allow the user to initiate a FUMO transaction by selecting an “Update Firmware” menu/button in the
following location:

Settings / System Update / Update Firmware

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00198

Windows devices must allow the user to initiate a FUMO transaction by selecting an “Update Firmware” menu/ button in the
following location:

Control Panel / Update Firmware applet

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00199

Blackberry devices must allow the user to initiate a FUMO transaction by selecting an “Update Firmware” menu/ button in the
following location:

Options / Mobile Network / Update Firmware

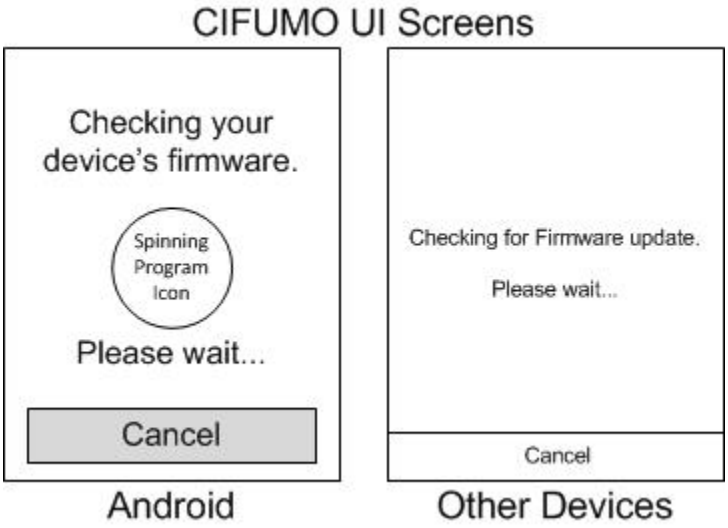
Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00188

When performing a CI-FUMO update, the following CI FUMO UI Screen must be displayed



Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00179

If both (binary package and download descriptor) are present, the firmware update process commences by displaying the FUMO Opt-In screen from OMA-SIMOTA-00190.

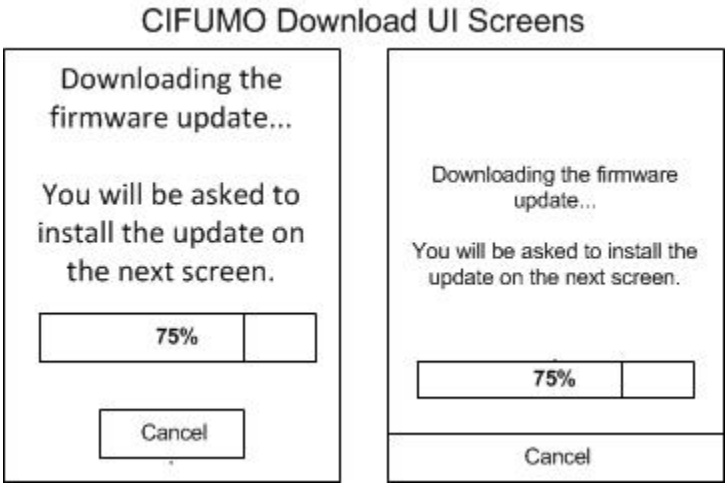
Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00189

When downloading an available package, the device must display the following FUMO Download UI Screen. This applies to both NI-FUMO and CI-FUMO.



Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00180

When the download automatically begins, the device must display the FUMO Download UI Screen in OMA-SIMOTA-00189.

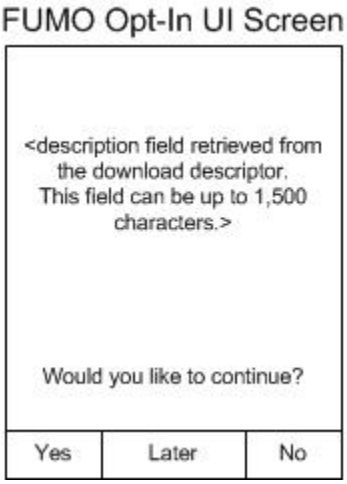
Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00190

Once the package is fully downloaded, the device must display the FUMO Opt-In Screen before installation.



Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00181

The device must support a <description> element up to 1,500 characters long. The device must display it to the user in the FUMO Opt-In UI screen in OMA-SIMOTA-00190.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00194

The Opt-In Screen displays the entire <description> field from the download descriptor and the prompt for installation. This screen must allow scrolling for long messages.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00195

If the user opts in to install the package by choosing Yes, the device must immediately terminate all processes and begin the installation.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00182

If the user opts out of the install by choosing No, the device must display the FUMO Reporting Status UI screen from OMA-SIMOTA-00192. The package must be saved on the device in case the user wants to install again later. If the user chooses “Update Firmware” again in the future, the device can launch directly into the FUMO Opt-In UI screen from OMA-SIMOTA-00190 because the package was saved and is immediately available.

Priority: Deprecated

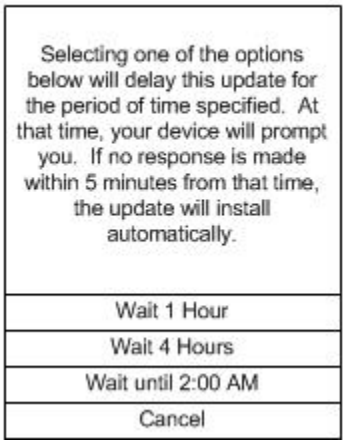
Category: Cat1

Device: Smartphone

OMA-SIMOTA-00191

If the user defers the install by choosing Later, the device must display the following UI screen.

FUMO Install Delay UI Screen



Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00183

If the user selects Wait 1 Hour, the device must wait one hour and then pop up the FUMO Opt-In UI screen from OMA-SIMOTA-00190. If the user then makes another selection, the appropriate action from OMA-SIMOTA-00195, OMA-SIMOTA-00182 or OMA-SIMOTA-00191 must be performed. If no selection is made within 5 minutes, the device must proceed to installing the firmware update.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00184

If the user selects Wait 4 Hour, the device must wait four hours and then pop up FUMO Opt-In UI screen from OMA-SIMOTA-00190. If the user then makes another selection, the appropriate action from OMA-SIMOTA-00195, OMA-SIMOTA-00182 or OMA-SIMOTA-00191 must be performed. If no selection is made within 5 minutes, the device must proceed to installing the firmware update.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00185

If the user selects Wait until 2:00 AM, the device must wait until 2:00 AM and then pop up FUMO Opt-In UI screen from OMA-SIMOTA-00190. If the user then makes another selection, the appropriate action from OMA-SIMOTA-00195, OMA-SIMOTA-00182 or OMA-SIMOTA-00191 must be performed. If no selection is made within 5 minutes, the device must proceed to installing the firmware update.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00186

If the user selects Cancel, the device must display FUMO Opt-In UI screen from OMA-SIMOTA-00190.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00187

After an update attempt – success or failure – the device must report its final state immediately to the OMA DM server. The FUMO Reporting Status UI screen from OMA-SIMOTA-00192 must be displayed during this Alert back to the network.

Priority: Deprecated

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00192

The FUMO Reporting Status screen should be displayed immediately on power-up following the installation attempt.

FUMO Reporting Status UI Screen

Priority: Deprecated

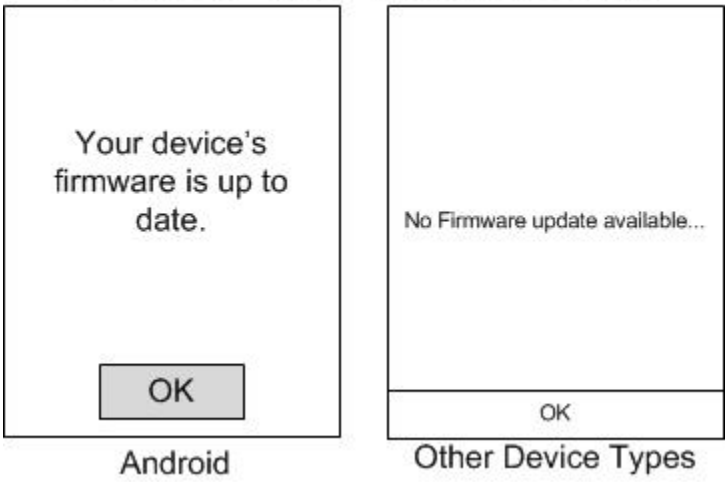
Category: Cat1

Device: Smartphone

OMA-SIMOTA-00193

The device must inform the user that no updates are available. This is defined by an “empty session” where the DM server does not perform any Replace commands and ends the management session. The device must display the following UI screen in this instance. The device will NOT receive a UI alert from the server indicating no updates are available.

CIFUMO No Update AvailableUI Screens



Priority: Deprecated

Category: Cat1

Device: Smartphone

8 Additional Management Objects

8.1 Chameleon

Sprint will use a collection of objects to customize a device over-the-air at the point of activation. The details of these nodes are described below and in the [Sprint DDF].

The CustID node in the customization tree will determine if the device is customized correctly or not customized yet. If the server reads the CustID node and it is not set to the correct value, the customization process will restart from the first node. The CustId values are assigned by the server to each customization package that is loaded (for each make/model).

OMA-SIMOTA-00203

For the nodes that use the B64 format, the OEM must convert the raw binary file into Base64 (B64) format that the device can recognize. Each file should be encoded in B64 format as defined by RFC2045.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00204

All customization nodes MUST be stored in a manner that will not allow them to be cleared or reset during a FOTA update. This MUST allow even the PRI settings to be changed without impacting the OMA payload or requiring a Google Factory Data Reset.

Priority: Must

Category: Cat1

Device: Smartphone

8.2 LTE Enablement Management Object

Sprint's 4G strategy includes the use of a LTE network. During activation (HFA) or profile updates (NIDC or CIDC), the payload for a dual-mode device may include the following management objects related to LTE.

OMA-SIMOTA-00205

The device must support NV items for LTE_Enabled, eHRPD_Enabled, and LTE_Forced.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00206

The device must populate the LTE_Forced NV item with the value received in the ./LTE/Service/Forced node.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00207

The device must populate the LTE_Enabled NV item with the value received in the ./LTE/Service/Enabled node.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00208

The device must populate the eHRPD_Enabled NV item with the value received in the ./CDMA/EHRPD/Enabled node.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00209

If the LTE_Forced NV item equals 1, the device must grey out the user preference menu item and not allow the user to change the setting.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00210

If the LTE_Forced NV item equals 0, the device must use the PRI value or user setting.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00211

The device must allow the user to enable or disable the LTE radio if the ./LTE/Service/Forced flag is disabled (set to ‘0’).

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00212

The device must support up to eight (8) APN records for use on LTE.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00213

The device must receive and store all eight APN records in non-volatile memory in the UE during a management session with the OMA-DM server.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00214

The device must parse the fields of each APN node and store the data in a manner that is most efficient for use.

Note, it is permitted for the device vendor to load the APN information into RAM directly from the DM Tree. It is also permitted for the device vendor to maintain an optimized table or database of APN information based on the information written to the ./LTE/APN/* nodes.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00215

The device must parse the nine (9) fields of each APN record in the following format:

Comma separated fields
<APN Data>,<APN Name Type>,<APN NI>,<PDN Type>,<Inactivity Timer>,<RAT Type>,<Authentication Type>,<Username>,<Password>

The <APN Data> field will be set to ‘1’ when there is APN data. It will be set to ‘0’ when there is no APN data. When set to ‘0’ all other fields in the record will be blank and there won’t be any commas. If the <APN Data> field is set to ‘0’, any entries in the APN table for that APN record must be deleted.
The <APN Name Type> will be a string describing the type of usage allowed. Examples include “ota,” “internet” or “pam.”
The <APN NI> will be a string value.
The <PDN Type> will be string indicating what type of IP connectivity is allowed. Examples include “IPv4,” “IPv6” or “IPv4v6.”
The <Inactivity Timer> is an integer representing the number of minutes.
The <RAT Type> is a string value indicating which Radio Access Technology is allowed for that particular APN record. Examples include “LTE,” “EHRPD” or a combination “LTE|EHRPD.”
The <Authentication Type> is a string value indicating what authentication scheme is used for a particular APN record. This field can be null. Examples include “PAP.”
The <Username> is a string value containing the username to be used when accessing a particular APN. This field can be null.
The <Password> is a string value containing the password to be used when accessing a particular APN record. This field can be null.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00216

The device must support any combination of up to eight APN records. The records may not be contiguous. Example, any given device may get APN/0, APN/2 and APN/3 while APN/1 will be skipped and set to '0'.

LTE APN Payload Examples (Informational Only)
See the [Sprint DDF] for specific details regarding the nodes.

Example Scenario A – Provisioning a Boost LTE device with OTA, Internet, PAM APN settings
<LTE>

<LTE_ENABLEMENT>1</LTE_ENABLEMENT>
<FORCE_FLAG>0</FORCE_FLAG>
<APN_0>1,ota,ota,IPv4v6,15,LTE|EHRPD,null,null,null</APN_0>
<APN_1>1,internet,isp.boost,IPv4v6,60,LTE|EHRPD,null,null,null</APN_1>
<APN_2>1,pam,pam.boost,IPv4v6,60,LTE|EHRPD,PAP,jfarme04,password</APN_2>
<APN_3>0</APN_3>
<APN_4>0</APN_4>
<APN_5>0</APN_5>
<APN_6>0</APN_6>
<APN_7>0</APN_7>

</LTE>

Example Scenario B – Updated provisioning payload with a removed PAM APN setting.
<LTE>

<LTE_ENABLEMENT>1</LTE_ENABLEMENT>
<FORCE_FLAG>0</FORCE_FLAG>
<APN_0>1,ota,ota,IPv4v6,15,LTE|EHRPD,null,null,null</APN_0>
<APN_1>1,internet,isp.boost,IPv4v6,60,LTE|EHRPD,null,null,null</APN_1>
<APN_2>0</APN_2>
<APN_3>0</APN_3>
<APN_4>0</APN_4>
<APN_5>0</APN_5>
<APN_6>0</APN_6>
<APN_7>0</APN_7>

</LTE>

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00217

The device must support an APN record of up to a total of 500 characters in length.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00218

The device must ONLY use the OTA APN for OMA DM transactions over LTE or eHRPD.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00219

The device must explicitly request the OTA PDN when connecting to perform an OMA request.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00220

An LTE only device MUST support a 30 day polling interval. At the end of this interval, the device must perform a CIDC~~., and CIFUMO.~~

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00277

If the device has active APN's of the PDN type in the OMA payload, the client must update the active record instead of creating a new one.

Priority: Must

Category: Cat1

Device: Smartphone

8.3 Service Plan Awareness Management Object

The nodes for service plan awareness will be part of the activation payload during HFA/CIDC and may be changed via NIDC. The Device Capabilities Management specification defines the behavior of the device in regard to each of the following settings. This document only defines the updateable nodes and their format.

OMA-SIMOTA-00221

The following table is a reference for correctly implementing SPA. Please note that the enabled node for the roaming guards is for a bar on roaming. So if ./SPA/BarDomDataRoaming is Y, then domestic data roaming should be blocked.

Table: SPA Table

OMA DM Node	OMA Node Value	Status	UI Display	User Configurable
./SPA/DomDataGuard/Enabled	N	Guard Disabled	No Check	
	Y	Guard Enabled	Check	
./SPA/DomDataGuard/Forced	N			Y
	Y			N
./SPA/BarDom-DataRoaming/Enabled	N	Roaming Enabled	Check	
	Y	Roaming Disabled	No Check	
./SPA/BarDom-DataRoaming/Forced	N			Y
	Y			N
./SPA/DomVoiceGuard/Enabled	N	Guard Disabled	No Check	
	Y	Guard Enabled	Check	
./SPA/DomVoiceGuard/Forced	N			Y
	Y			N
./SPA/Bar-DomVoiceRoaming/En-abled	N	Roaming Enabled	Check	
	Y	Roaming Disabled	NoCheck	
./SPA/Bar-DomVoiceRoaming/Forced	N			Y
	Y			N
./SPA/IntlDataGuard/En-abled	N	Guard Disabled	No Check	
	Y	Guard Enabled	Check	
./SPA/IntlDataGuard/Forced	N			Y
	Y			N
./SPA/BarIntlDataRoam-ing/Enabled	N	Roaming Enabled	Check	
	Y	Roaming Disabled	No Check	

./SPA/BarIntlDataRoaming/Forced	N			Y
	Y			N
./SPA/IntlVoiceGuard/Enabled	N	Guard Disabled	No Check	
	Y	Guard Enabled	Check	
./SPA/IntlVoiceGuard/Forced	N			Y
	Y			N
./SPA/BarIntlVoiceRoaming/Enabled	N	Roaming Enabled	Check	
	Y	Roaming Disabled	No Check	
./SPA/BarIntlVoiceRoaming/Forced	N			Y
	Y			N
./SPA/BarLTEDataRoaming/Enabled	N	Roaming Enabled	Check	
	Y	Roaming Disabled	No Check	
./SPA/BarLTEDataRoaming/Forced	N			Y
	Y			N
./SPA/LTEDataRoamGuard/Enabled	N	Roaming Enabled	Check	
	Y	Roaming Disabled	No Check	
./SPA/LTEDataRoamGuard/Forced	N			Y
	Y			N
./SPA/BarIntlLTEDataRoaming/Enabled	N	Roaming Enabled	Check	
	Y	Roaming Disabled	No Check	
./SPA/BarIntlLTEDataRoaming/Forced	N			Y
	Y			N
./SPA/IntlLTEDataRoamGuard/Enabled	N	Roaming Enabled	Check	
	Y	Roaming Disabled	No Check	
./SPA/IntlLTEDataRoamGuard/Forced	N			Y
	Y			N

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00222

The client will write any changes to these nodes into the tree, but the device vendor is responsible for implementing the controls for the various services. For example, the client will write the International Roaming block nodes but the device vendor must implement the logic for preventing international roaming usage per the [Sprint DevCap] specification.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00223

The configuration store that contains the tree must be accessible by the components that must read data from it. The DM Tree must allow all components of the device to access values of the nodes.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00224

The device vendor must make the components aware of changes to these nodes in the tree. This can be accomplished by reading the tree periodically, pushing notifications from the tree to interested applications, or any other means.

Priority: Must

Category: Cat1

Device: Smartphone

8.4 Band Class Management Object

OMA-SIMOTA-00226

The device must only reboot if the value of the ./CDMA/BC10 and/or ./CDMA/SO68 nodes change and it cannot support applying the updates with a radio reset.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00227

If the value in the ./CDMA/BC10 node changes on the device after a device configuration, the device must perform a full reboot or radio reset after the session completes.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00228

If the value in the ./CDMA/SO68 node changes on the device after a device configuration, the device must perform a full reboot or radio reset after the session completes.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00225

If the device supports either of the ./CDMA/BC10 or ./CDMA/SO68 nodes, it must support both of them.

Priority: Must

Category: Cat1

Device: Smartphone

8.5 1x Advanced Management Object

OMA-SIMOTA-00229

If the value in the ./CDMA/SO73/COP0 node changes on the device after a device configuration, the device must perform a full reboot or radio reset after the session completes.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00230

If the value in the ./CDMA/SO73/COP1to7 node changes on the device after a device configuration, the device must perform a full reboot or radio reset after the session completes.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00231

If the value in the ./CDMA/1xA/Enabled node changes on the device after a device configuration, the device must perform a full reboot or radio reset after the session completes.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00232

The device must only reboot if the value of the ./CDMA/ SO73/COP0, ./CDMA/ SO73/COP1to7 and/or ./CDMA/1xA/ Enabled nodes change and the change cannot be applied with a radio reset.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00233

If the device supports any one of these ./CDMA/ SO73/COP0, ./CDMA/ SO73/COP1to7 and/or ./CDMA/1xA/ Enabled nodes, it must support all three.

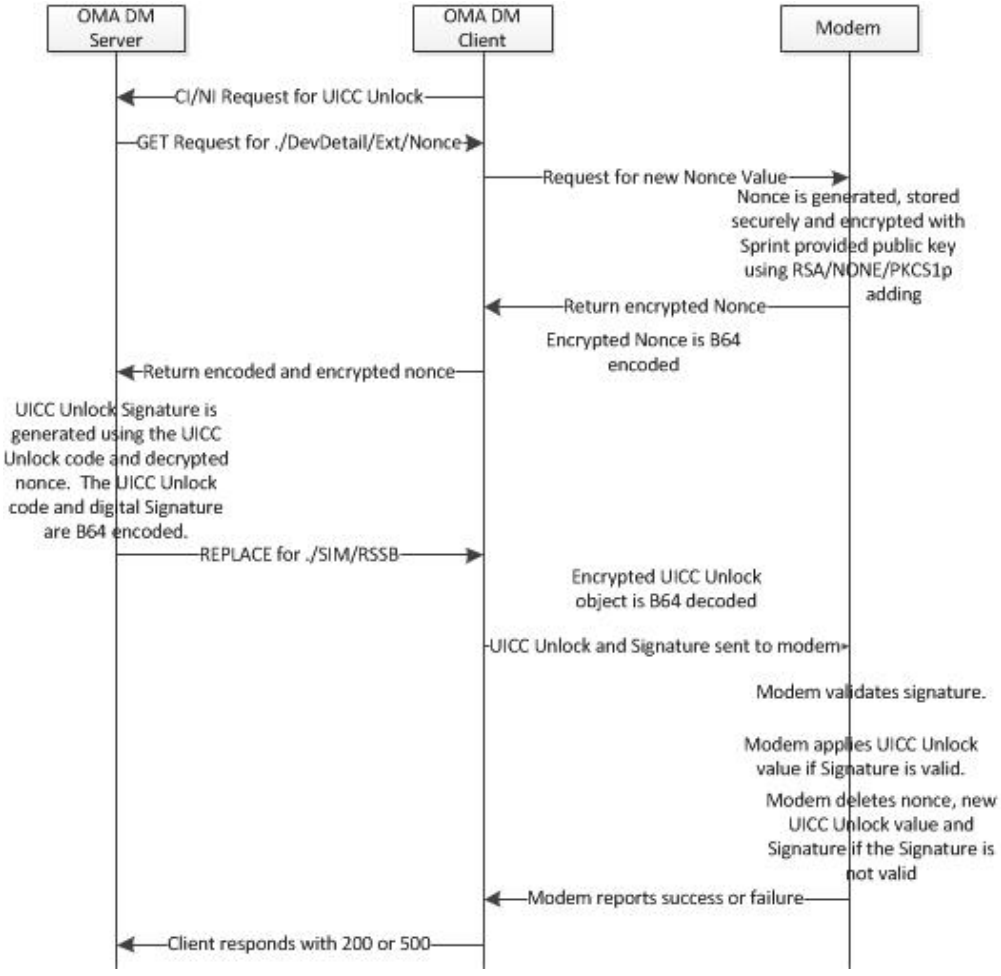
Priority: Must

Category: Cat1

Device: Smartphone

8.6 UICC Unlock Service

The SIM lock service will enable Care to send an NI request to the device that will allow the use of a non-Sprint SIM.



OMA-SIMOTA-00280

A Sprint UICC is defined as having an MCC/MNC of 310120 or 312530 in the IMSI.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00235

The ./SIM/RSSB node MUST NOT be updatable by any method other than OMA-DM.

Note: Sprint expects the OEM's to test that this unlock method is secure and is not updatable by ANY means other than Sprint's OMA DM server.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00234

The device must support an NI update to the ./SIM/RSSB node.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00282

The OMA Client MUST not respond to the server for a replace on the ./SIM/RSSB node until the object has been successfully sent to the modem and the modem has reported its success or failure to verify that it can authenticate the message.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00283

The UICC Unlock setting in the modem must be secure at all times.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00317

The OMA DM client must use the UICC Unlock URL from the OMA DM Server Configuration Table for all CI UICC Unlock requests. The OMA DM Server Configuration Table can be found in the OMA DM / FUMO EAP.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00318

The UICC Unlock requirements in Section 8.6 apply to all devices that support removable UICC's and eUICC profiles. If the device supports multiple UICC slots or a combination of embedded and removable UICC's/eUICC's, the SIM lock setting applies to ALL slots and profiles.

Priority: Must

Category: Cat1

Device: Smartphone

8.6.1 UICC Unlock UI

OMA-SIMOTA-00243

Android devices must allow the user to initiate a UICC Unlock transaction by selecting an “UICC Unlock” menu/ button in
the following location:

Settings / System Update / UICC Unlock

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00245

Windows devices must allow the user to initiate a UICC Unlock transaction by selecting an “UICC Unlock” menu/ button in
the following location:

Control Panel / UICC Unlock

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00246

Blackberry devices must allow the user to initiate a UICC Unlock transaction by selecting an “UICC Unlock” menu/ button in
the following location:

Options / Mobile Network / UICC Unlock

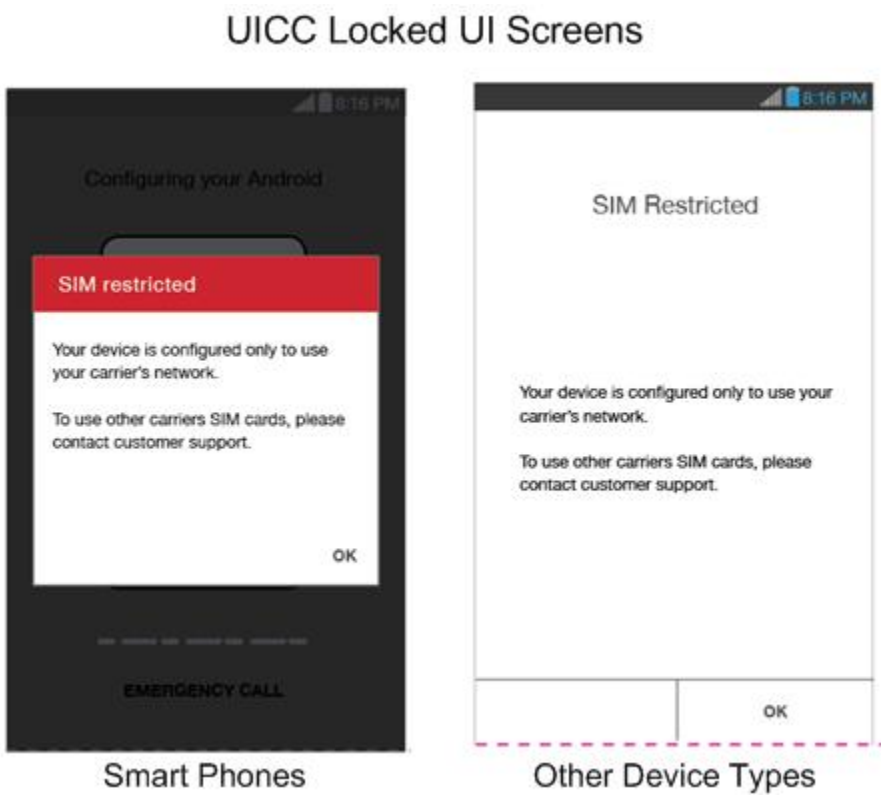
Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00237

If the server returns an empty session for a CI UICC Unlock request, a NULL value, or a UICC Unlock 0 for the ./SIM/RSSB node the following UI Screen must be displayed.



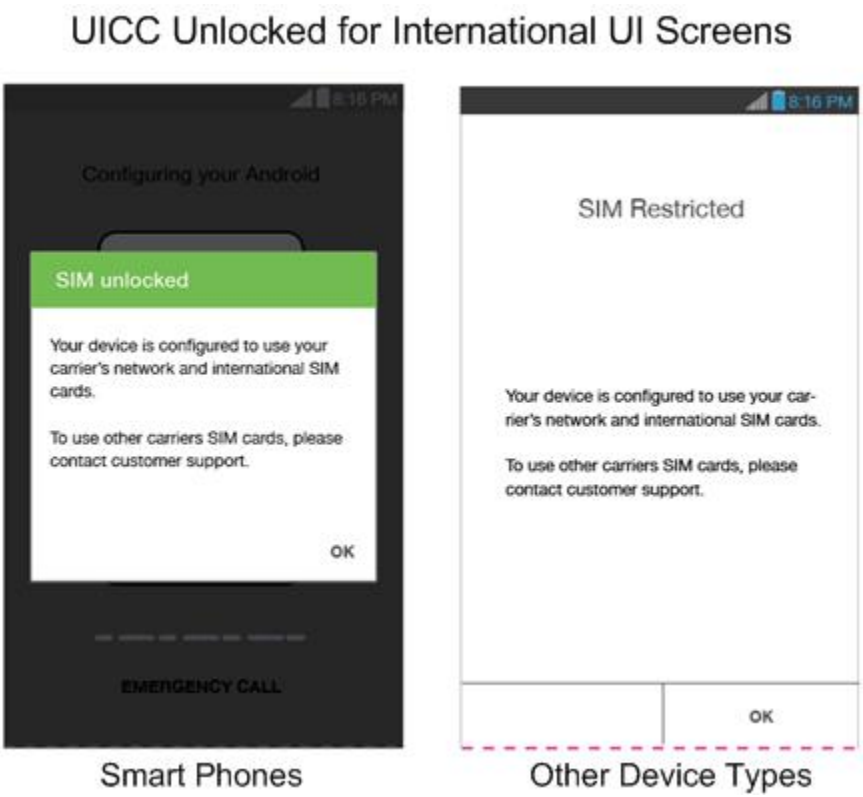
Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00239

If the server returns a UICC Unlock setting of 1 for the ./SIM/RSSB node, the following UI screen must be displayed.



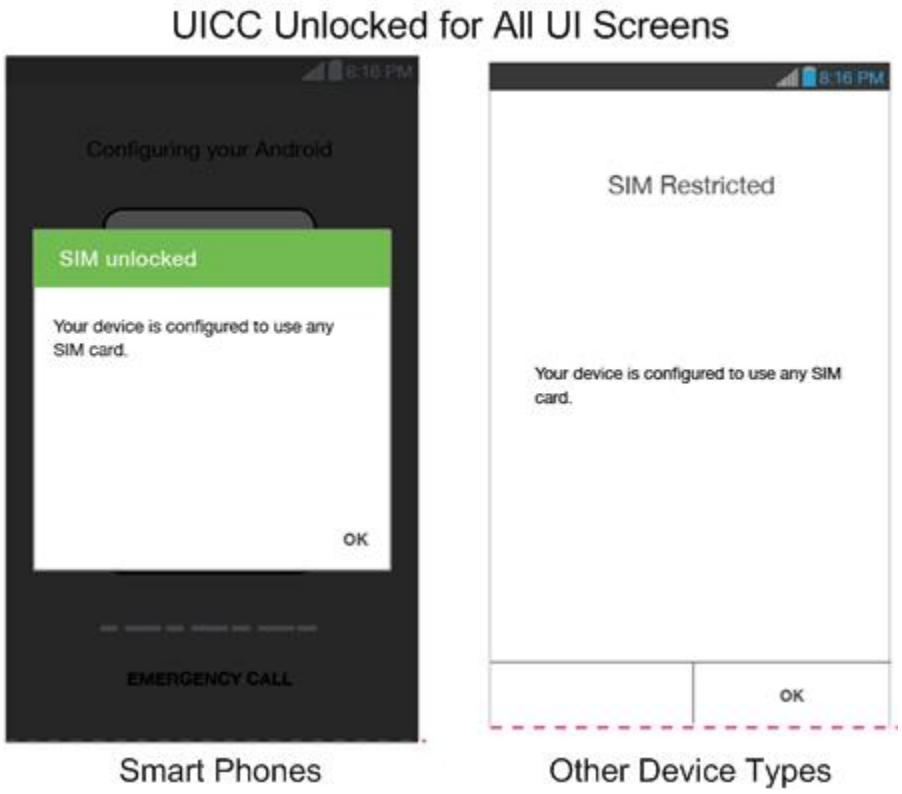
Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00242

If the server returns a UICC Unlock setting of 2 for the ./SIM/RSSB node, the following UI screen must be displayed.



Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00248

The settings menu item for UICC unlock must have subtext displaying the current lock state of the device.

For a ./SIM/RSSB UICC Unlock setting of 0, the subtext should display that the device is locked to a Sprint SIM only.

For a ./SIM/RSSB UICC Unlock setting of 1, the subtext should display that the device is locked to a Sprint or International SIM.

For a ./SIM/RSSB UICC Unlock setting of 2, the subtext should display that the device is unlocked for any SIM card.

Priority: Must

Category: Cat1

Device: Smartphone

8.6.2 UICC Unlock Values

OMA-SIMOTA-00236

If the UICC Unlock value for ./SIM/RSSB is 0, the device must only recognize and enable an inserted Sprint UICC. If a non-Sprint SIM is inserted when the UICC Unlock value in ./SIM/RSSB is 0, the device must not recognize or allow the SIM to be used.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00238

If the UICC Unlock value for ./SIM/RSSB is 1, the device must recognize and enable any inserted international (Not a USA MCC) SIM as well as a Sprint SIM.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00240

If the UICC Unlock value for ./SIM/RSSB is 1, the device must perform a CI request every 30 days using the 1226 alert string for SIM Lock. If the UICC Unlock value for ./SIM/RSSB is 0 or 2, the client must NOT poll.

Note: The OEM must provide a means to change the polling interval for testing.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00241

If the UICC Unlock value for ./SIM/RSSB is 2, the device must recognize any inserted UICC, International or Domestic.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00319

The device MUST be able to freely transition between UICC Lock states.

As an example, if the current UICC Unlock setting is 2, and the OMA DM server sends a 0, the device must re-lock to only supporting a Sprint UICC.

Priority: Must

Category: Cat1

Device: Smartphone

8.6.3 UICC Unlock Nonce

OMA-SIMOTA-00284

If the OMA client receives a GET request for the ./DevDetail/Ext/Nonce node the client must send a request to the modem for a new Nonce.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00285

When the modem receives a request from the OMA DM client for a nonce, the modem must generate a random nonce, append the MEID or IMEI to the end and store it securely. The same value (MEID or IMEI) must be used as what the OMA DM client is using as the device ID. If an MEID is used, it must be in Hex format and a 'Z' must be added to the end.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00286

The combined nonce must be a minimum of 80 bytes and a max of 100 bytes in length.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00287

The nonce must be in Hexadecimal or B64 format. The Hexadecimal or B64 formatted nonce is what will be used in Signature generation.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00288

Nothing outside of the modem must be allowed to read the nonce value that is being stored in the modem.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00289

The modem must then encrypt the nonce with the Sprint provided public key using RSA/NONE/PKCS1Padding.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00290

The encrypted nonce must then be provided to the OMA DM client. This encrypted nonce must ONLY ever be provided to the OMA DM client. The nonce must only ever be provided to the OMA DM client in an encrypted format.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00292

If the modem receives an object for the ./SIM/RSSB node but does not have a nonce saved securely, the object must be ignored and discarded.

Priority: Must

Category: Cat1

Device: Smartphone

8.6.4 UICC Unlock Signature

OMA-SIMOTA-00293

The UICC Unlock Signature will be created using [UICC Unlock Code][Nonce].

Example:

2aklsdskdjfalsdjfalskdjfalskdjfKDGSLDGNLSKDFLSKdnflansdfnaslslkdnfaslkdnfalskdfnaslkdf35850308003154Z

Where 2 is the UICC Unlock Code and aklsdskdjfalsdjfalskdjfalskdjfKDGSLDGNLSKDFLSKdnflansdfnaslslkdnfaslkdnfalskdfnaslkdf35850308003154Z is the nonce.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00294

The modem MUST be able to support hashing using SHA256 for the purpose of creating the digest for validating the UICC Unlock Signature.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00295

The modem MUST be able to support NONEWITHRSA for the purpose of validating the signature of the UICC Unlock Signature from the hashed digest.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00296

The modem MUST generate the hashed digest and perform the signature validation as two separate steps.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00297

The modem must validate the signature from the ./SIM/RSSB node before updating the UICC Unlock setting.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00298

If the signature is not valid, the new UICC unlock value must be ignored and the OMA DM client MUST return a 500 error code to the OMA DM server for the REPLACE command on the ./SIM/RSSB node. At this time the modem must also discard the nonce it has stored.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00299

The modem must validate the signature from the UICC Unlock payload that is saved in the modem against the nonce on every power on before applying the UICC Unlock setting.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00300

If the Signature validation is successful during power on, the modem must apply the UICC unlock setting from the ./SIM/RSSB node.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00301

If the Signature validation fails during power on, the modem must discard the UICC unlock setting from the ./SIM/RSSB node, Signature and Nonce then revert back to a locked to Sprint only state. If this occurs, the device must notify the user that the device is now locked to a Sprint UICC again.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00302

The content of the ./SIM/RSSB node will be [LOCK_CODE][SIGNATURE].

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00303

The LOCK_CODE will be the first byte of the B64 decoded value from the ./SIM/RSSB node.

Priority: Must

Category: Cat1

Device: Smartphone

8.7 Carrier Aggregation

OMA-SIMOTA-00249

If a Carrier Aggregation mode is enabled, and the device receives a new payload that does not contain the enablement for that mode, it must be disabled.

For example:

The client receives "41C,41D" for the ./LTE/CA/Enablement node in the OMA payload. The device would then enable 41C and 41D Carrier Aggregation modes. If later the device receives a new payload of "41C"for the ./LTE/CA/Enablement node, the device would then leave 41C enabled, but would disable 41D. If the device then received a new payload of "off" for the ./LTE/CA/Enablement node, it would disable all Carrier Aggregation modes.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00250

The node will be sent containing the Band Names to be enabled.
The node values will be comma delimited if more than band is to be enabled in the payload.

Please see requirement GTR-LTE_RF-00226 in the DM Bearer GTR for the full list of settings that must be supported.

For example, if only CA_41C is being enabled, the payload will be “41C”.
If CA_41C, CA_41A-41A and CA_1A-8A are all being enabled, the payload will be “41C,41A41A,1A8A”.

Priority: Must

Category: Cat1

Device: Smartphone

9 Hidden Menus

9.1 ##UPDATE#

OMA-SIMOTA-00251

The device must support the ##UPDATE# code.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00252

Once ##UPDATE# is entered, the device must perform a CI DC ~~followed by a CI FUMO~~.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00253

The device must perform all steps in the foreground using the appropriate UI screens for each step. For example, the CIDC portion would use the UI screen defined for CIDC.

Priority: Must

Category: Cat1

Device: Smartphone

9.2 ##OMANI#

OMA-SIMOTA-00254

The device must support the ##OMANI# code.

Priority: Optional

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00255

Once ##OMANI# is entered, the device must perform a connection to the OMA server as if it is responding to a generic alert from an NIA. The client must respond as if the UI mode is set to Informative.

Priority: Optional

Category: Cat1

Device: Smartphone

9.3 ##OMADM#

OMA-SIMOTA-00256

The device must support a hidden menu, ##OMADM#, that will allow a user, after entering the device MSL, to update the OMA DM Server Indicator setting.

Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00257

The device must support a table as define by Sprint that defines the ./DMAcc and Sprint Specific values for all Sprint OMA DM environments.

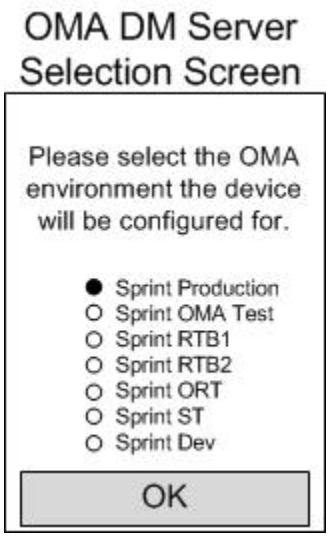
Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00258

After a user has entered the MSL for ##OMADM#, the device must display a menu that displays the Server name for each entry in the routing table.



Priority: Must

Category: Cat1

Device: Smartphone

OMA-SIMOTA-00259

Once the user selects the Server Name from the UI Screen and taps OK, the OMA DM Server Indicator value must be changed to the appropriate setting from the Server Routing Table in the PRI.

Example: If the OMA DM Server Indicator value is currently set to 1 and the user selects Sprint RTB 2 and taps OK, the OMA DM Server Indicator value must be changed to 4, and the client must now use the settings for Server Indicator 4.

Priority: Must

Category: Cat1

Device: Smartphone

11 Mobile Broadband

12 Appendix

12.1 GSS

OMA-SIMOTA-00276

The OEM must fill in the GSS (GTR Support Sheet) for clarification of the device behavior.

Priority: Must

Category: Cat1

Device: Smartphone