Reference : AAANNN_ATP	Release : 1 . 0
(Printed copy not controlled: verify the version before using)	Pages : 24

Acceptance Test Plan

For LinqUs Device Manager | Device Detection

	Name	Role	Date (yyyy/mm/dd)	Signature
Issued by	Rodrigo Pliego	Integrator	2010/12/16	
Verified by				
Approved by				

Distribution list			
Name	**Role or Function**	**Name**	**Role or Function**
Miguel Serrano	Gerente de Proyecto	Johan Alemán	Gerente de Proyecto
Rodrigo Pliego	Ingeniero Integrador	Luis Diego Hidalgo	Solution Architect
Juan Carlos Cuevas	Gerente Integración	Macsee Vallejos	Ingeniero de Operación

21/12/2010

Document Releases

Release (X.Y)	Date (yyyy/mm/dd)	Author	Modifications
1.0	2010/12/16	Rodrigo Pliego	Cellphone Models

Table of content

2/12/2010

1 Introduction

This document describes the set of technical tests to be executed for the approval of the LinqUs Device Manager solution. Device Manager solution includes Device Manager platform, responsible for message formatting, for subscriber, handset and services management; and the Device Detection platform, responsible for the detection of changes of handsets for the subscribers and to trigger Device Manager platform.

1.1 References

Document Name	Description	Organization	Version and date	Ref

1.2 Conventions

1.2.1 Icons

This sign in the document margin indicates **limitations**.


This sign in the document margin indicates a **rule**.


This sign in the document margin indicates **information**.

1.2.2 Colors

Blue mark Word to be defined
Red mark Field to be updated

1.2.3 Terminology

ADN Abbreviated Dialing Numbers (Phonebook)
GSM Global System for Mobile Communication
ME Mobile Equipment
MO Mobile Originated
MT Mobile Terminated
N/A Not Applicable
OTA Over The Air
SIM Subscriber Identity Module
FDN Fixed Dialing Number
SDN Services Dialing Number
SPN Service Provider Name
ICCID Sim serial number of the card
IMSI International Mobile Subscriber Identity

21/12/2010

MSISDN	Mobile Station Integrated Services Digital Network number
SMSC	Short Message Service Center
PLMN	Public Land Mobile Network
FPLMN	Forbidden PLMN
MLS	Microsoft Live Server
TOU	Terms of User
WLS	Windows Live Server

2 Responsibilities

During the acceptance phase, the teams are working together with the following responsibilities:
- **OPERATOR** is in charge of the functional testing and the system administration testing.
- Gemalto provides a functional and a technical support to **OPERATOR**.

The project managers mutually qualify the test results and sign the ATP, acknowledging the fact that the product that was delivered to **OPERATOR** is according to the requirements.

The problems encountered during the acceptance are necessarily reported to:
- Gemalto project manager,
- **OPERATOR**'s project manager.

Each problem identified during the acceptance will be described in the anomaly sheet supplied at the end of this document. The person responsible of the project follow-up contacts the people involved in solving the problem.

Rule 1: This ATP should be signed at all pages by the integrator and the client who executed it.
Rule 2: The original ATP signed should be completely scanned and it images should be included in a pdf that must be archived within its project.
Rule 3: The original ATP signed should be sent to the GSA's financial controller by mail.

3 Means Required for Tests

These acceptance tests will be processed on OPERATOR production platform after the software installation by GEMALTO.

No application or software other than those provided by GEMALTO will be running on this platform during test sessions.

Only the connections needed for the tests will be allowed during the acceptance period.

4 Anomaly Classification

There is a distinction between the different kinds of anomaly:

- **Minor Anomaly:** An anomaly that does not have an effect on the functioning of the application.
- **Major Anomaly:** An anomaly that has an effect on the functioning of the application.
- **Blocking Anomaly:** Anomaly that has an effect on the functioning of the application. Its detection does not allow a continuation of the acceptance. The acceptance should be re-planned once the anomaly has been corrected.

5 Handset List

During the acceptance phase, the handsets to run the tests are the ones bellow:

Manufacturer	Model	IMEI
Nokia	5800d	359348/02/310893/9
	-	-
	-	-
	-	-
Sony Ericsson	W705a	35180703-520869-6
	-	-

6 The Acceptance Procedure List

6.1 Preliminary Tests

6.1.1 OTA Manager CCI Access

Function verified	Connect on OTA Manager Customer Care Interface
Pre requisites	The user and password to log in into OTA Manager.
Test directions	Use a browser with the URL: http://<ota_ip_address>:8080/CCI Enter an account and password and login (admgemalto/*******) to the platform. Perform this test with all Card Manager Instances.
Expected output	LinqUS OTA Manager Login window is displayed. *If you register a valid account then a welcome window is displayed.*
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ***Anomaly Sheet Ref :*** ☐ **Not Blocking**

6.1.2 SMSC Reconnection

Function verified	Reconnection to the SMSC
Pre requisites	Access to the OTA Manager GUI.
Test directions	The SMSC module in Device Manager includes an automatic process of reconnection to the SMSC. Any network failure will be followed by a new connection process in less than **n** minutes (Device Manager parameter). 1. SMSC administrator should kill one connection. 2. The delay depends of the TCP/IP default time-out values. 3. Visualize the Device Manager status – the SMSC connection is lost and SMSC children processes are down.

	4. The connection is up in less than **n** minutes – view Device Manager status. Perform this test also with Device Detection module.
Expected output	*The connection to the SMSC has to be automatically restarted when the network is available again.*
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ☐ **Not Blocking** ***Anomaly Sheet Ref :***

6.2 Setting Set Tests

The setting management aims at provisioning or modifying some service setting sets in the product. These setting sets are composed of properties downloaded on the handset to active the corresponding service. The product manages the following service setting sets:

- MMSGPRS
- WAPGPRS

Some setting parameters are generic whereas others are specific to a subscriber.

The different settings have the following states:

_ Untested
_ Tested
_ Active
_ Disabled

Some transitions between these states are available. The setting sets can be modified only in the "Untested" state whereas they can be deleted in the "Untested" and "Disabled" states.

A user with an administrator profile can provide the management of the different setting sets. The customer care and the subscriber have the access to active setting sets only in order to download them by a provisioning transaction or top view their parameter values. The "Untested" and "Tested" setting sets are available by the administrator for test usage.

6.2.1 Setting Set Creation

This procedure aims at checking the setting set provisioning of this services available on the product:

- WAP Browsing on GPRS
- MMS on GPRS

Each setting set creation generates an XML file under the folder defined by the GDM parameter "GENERAL - SETTING_SET_LOCATION".

Function verified	**New service setting set provisioning by using the GUI interface**
Pre requisites	Access to the OTA Manager GUI. The profile used for the execution is an administrator profile with the "Setting Set Management" and the "Setting Set Viewing" access rights.
Test directions	1. Setting Set Creation:

	> Select the item "Setting Set Management" and then "Settings / Create". > Select the WAPGPRS service. > Insert a name for the new setting set. > Click on the "Create" button. > Fulfil all fields of the "WAP GPRS settings description" window. > Click on the "Create" Button. 2. Setting Set Viewing: > Click on the "Search" button. > Select the setting you have just created. > Click on the "View" button. > Visualise and check the different properties of the setting definition. > Click on the "Back" button to come back to the setting list.
Expected output	*# The "Setting search" window is active with the new setting set name in the label field.* # The different properties displayed in the "View" window correspond to those inserted in the previous steps. *# An XML file is generated after the setting set creation.*
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ☐ **Not Blocking** ***Anomaly Sheet Ref :***

6.2.2 Setting Set Deletion

This test aims at verifying that the service setting set deletion is possible if it is used or not (by a subscriber account) and only if the state of the setting set is "Untested" or "Disabled".

The deletion can be done by service setting set. There is no batch loading capability. At the end of this procedure execution, the report retrieving each action done with the product is analysed.

Each setting set deletion deletes the XML file generated during the setting set creation under the folder defined by the GDM parameter "GENERAL - SETTING_SET_LOCATION".

Function verified	**Service setting set deletion on the product through Device Manager CCI**
Pre requisites	Access to the OTA Manager GUI. The profile used for the execution is an administrator profile with the "Setting Set Management" and the "Setting Set Viewing" access rights.
Test directions	1. Setting Set Deletion: > Select the item "Setting Set Management" and then "Setting / Search For". > Create in the "Setting search" window a request to select the 'Untested' setting sets. > Click on the "Search" button to launch the research. > Select in the setting set list a setting set. > Click on the "Delete" button to delete the selected device. > Click on the "Cancel" button to cancel the action. > Click on the "Delete" button to delete the selected device. > Click on the "OK" button to confirm the deletion. > Click on the "Search" button to launch the research again. 2. Execute the step 1 to delete other setting sets: > One setting set in the "Tested" state. > One setting set in the "Active" state.

	> One setting set in the "Disabled" state.
Expected output	# The "Setting list" window is displayed without the deleted setting set. *# The XML file generated at the setting set creation is deleted.* # The setting sets in the "Tested" and "Active" states are not deleted. # The setting set in the "Disabled" state is deleted. *# For each setting set deleted, the corresponding XML file is deleted.*
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ☐ **Not Blocking** ***Anomaly Sheet Ref :***

6.2.3 Setting Set State Management

A setting set can have one of the following states:
- "Untested" (available for an administrator during the test phase)
- "Tested" (available for an administrator during the test phase)
- "Active"
- "Disabled"

The setting sets with the states "Tested", "Active" and "Disabled" are not updateable.
Only the "Untested" and "Disabled" setting sets can be deleted from the product.
This procedure checks the different life cycle of a setting set with the following transitions:
- "Untested" > "Tested" > "Active" > "Disabled".
- "Untested" > "Disabled".

In the same time, the test verifies that the customer care or the subscriber sees only the setting sets with the "Active" status whereas the administrator sees all existing setting sets. Each setting set modification updates the XML file generated at the setting set creation under the folder defined by the GDM parameter "GENERAL - SETTING_SET_LOCATION".

Function verified	**Setting set state management through Device Manager CCI**
Pre requisites	Access to the OTA Manager GUI. The profile used for the execution is an administrator profile with the "Setting Set Management" and the "Setting Set Viewing" access rights.
Test directions	1. Setting set modification: > Select the item "Setting Set Management" and then "Setting / Search For". > Create in the "Setting search" window a request to select an existing "Untested" setting set. > Click on the "Search" button to launch the research. > Select in the setting list a setting set. > Click on the "Update" button. > Modify the state of the selected setting set to "Tested". > Click on the "Update" button. 2. Setting set viewing: > Click on the "View" button. > Visualise and check the different properties of the setting set definition. > Click on the "Back" button to come back to the setting list. 3. Execute the steps 1 and 2 to update other setting set states:

	> An "Untested" service to "Active". > A "Tested" service to "Active". > An "Active" service to "Disabled". > A "Disabled" service to "Active". > An "Untested" service to "Disabled". > A "Tested" service to "Disabled". > An "Active" service to "Tested". > An "Active" service to "Untested". > A "Disabled" service to "Untested". > A "Disabled" service to "Tested".
Expected output	*# The "Setting list" window is active with the modified setting set in the label field.* # Only the state of the setting is modified to "Tested" due to the previous step. # For the 4 first transitions, the modification is executed safely but during the modification action, a message appears to warn that a modification is available only for the state. # For the other transitions, the modification is not executed and an error message appears because the transition is not available.
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ***Anomaly Sheet Ref :*** ☐ **Not Blocking**

6.3 Subscriber Tests

The subscriber handset management deals with the subscribers of the telecom operator. The product manages these subscribers by its MSISDN only. A subscriber creation needs the following elements useful for the product:

- MSISDN
- IMSI
- Subscriber state (activated/deactivated)
- Current device ("none" is allowed)
- Allowed service list with the service name, the values of user dependent parameters and the configuration status

Each subscriber can be linked to a group. The maximum number of different groups for a subscriber is 32 groups. The different group names are defined in the file of the platform.

The product must manage an history of the actions done on a specific subscriber with the following elements:

- A unique transaction reference
- MSISDN
- Subscriber group
- Action date
- Request issuer name
- List of provisioned services
- Handset reference

This history can be visualized, activated or deactivated and implements a purge mechanism.

6.3.1 Subscriber Handset Creation

This procedure aims at checking the possible links between MSISDNs, IMSIs, handset types and authorized services. The product must generate alarms if the subscribers already exist or if the creation is impossible. This test checks the alarm generation. For each subscriber, a report is generated.

Function verified	**New Subscriber handset provisioning by using Device Manager CCI**
Pre requisites	Access to the OTA Manager GUI. The profile used for the execution is an administrator profile with the "Setting Set Management" and the "Setting Set Viewing" access rights. Several handsets must be already provisioned in the platform. Several groups of subscriber handsets must be already provisioned in the platform.
Test directions	1. Subscriber Creation: > Select the item "Subscriber Management" and then "Subscriber / Create". > Fulfil all fields concerning the subscriber properties as its MSISDN, IMSI (optional), the linked groups and its current handset. > Add several subscribed services and several service configurations. (See example of data in attached file). > Click on the "Create" Button. 2. Subscriber Viewing: > Click on the "Search" button. > Select the subscriber > Click on the "View" button. > Visualise and check the different properties of the subscriber. > Click on the "Back" button to come back to the device list.
Expected output	*# The "Subscriber search" window is active with the new subscriber in the MSISDN field.* # The different properties displayed in the "View" window correspond to those inserted in the previous steps.
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ***Anomaly Sheet Ref :*** ☐ **Not Blocking**

6.3.2 Subscriber Handset Search

The criteria to search a handset are displayed above:

- MSISDN
- Handset manufacturer and/or model
- Service
- Subscription

The product displays the results of the researches with a list of subscriber. It is also possible to create requests based on several criteria in the same time.

Function verified	**Subscriber handset search by using Device Manager CCI**
Pre requisites	Access to the OTA Manager GUI.

	The profile used for the execution is an administrator profile with the "Setting Set Management" and the "Setting Set Viewing" access rights. Several handsets must be already provisioned in the platform. Several groups of subscriber handsets must be already provisioned in the platform.
Test directions	1. Subscriber Search: > Select the item "Subscriber Management" and then "Subscriber / Search For" > Create in the "Subscriber search" window a request to select one existing subscriber by its MSISDN. > Click on the "Search" button to launch the research. > Select in the subscriber list the subscriber. 2. Subscriber Viewing: > Click on the "View" button. > Visualise and check the different tabs of the subscriber definition. > Click on the "Back" button to come back to the subscriber list. 3. Subscriber Search: > Select the item "Subscriber Management" and then "Subscriber / Search For" > Create in the "Subscriber search" window a request to select one or several existing subscriber by its current handset. > Click on the "Search" button to launch the research. > Select in the subscriber list several subscribers. 4. Subscriber Viewing: > Click on the "View" button. > Visualise and check the different tabs of the subscriber definition. > Click on the "Back" button to come back to the subscriber list. 5. Subscriber Search: > Select the item "Subscriber Management" and then "Subscriber / Search For" > Create in the "Subscriber search" window a request to select one or several existing subscriber by its subscribed service. > Click on the "Search" button to launch the research. > Select in the subscriber list several subscribers. 6. Subscriber Viewing: > Click on the "View" button. > Visualise and check the different tabs of the subscriber definition. > Click on the "Back" button to come back to the subscriber list. 7. Subscriber Search: > Select the item "Subscriber Management" and then "Subscriber / Search For" > Create in the "Specific subscriber search" window some requests to select one or several existing subscribers according to different criteria based on the MSISDN value, the subscriber state, the linked groups or services and the device. > Click on the "Search" button to launch the research. > Select in the subscriber list several subscribers. 8. Subscriber Viewing: > Click on the "View" button. > Visualise and check the different tabs of the subscriber definition. > Click on the "Back" button to come back to the subscriber list.
Expected output	# The "Subscriber list" window is active. # The MSISDN value must correspond to the value inserted in the request. # The "Subscriber list" window is active. # The current handset of the selected subscribers must be in accordance with the

	device selected in the request. # The "Subscriber list" window is active. # The "Subscriber list" must contain subscribers with the selected service in the subscription. # The subscribed service list must contain the service selected in the request. # The "Subscriber list" window is active. # The "Subscriber list" must contain subscribers corresponding to the criteria concerning the MSISDN values, the linked groups and the subscriber state. # The different properties must be in accordance with the different criteria inserted in the request.
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ***Anomaly Sheet Ref :*** ☐ **Not Blocking**

6.3.3 Subscriber Handset Deletion

Function verified	**Subscriber handset deletion by using Device Manager CCI**
Pre requisites	Access to the OTA Manager GUI. The profile used for the execution is an administrator profile with the "Setting Set Management" and the "Setting Set Viewing" access rights. Several handsets must be already provisioned in the platform. Several subscriber handsets must be already provisioned in the platform in order to be modified.
Test directions	1. Subscriber Deletion: > Select the item "Subscriber Management" and then "Subscriber / Search For" > Create in the "Subscriber search" window a request to select one or several existing subscribers. > Click on the "Search" button to launch the research. > Select in the subscriber list an inactive subscriber. > Click on the "Delete" button to delete the selected subscriber. > Click on the "Cancel" button to cancel the action. > Click on the "Delete" button to delete the selected subscribers. > Click on the "OK" button to confirm the deletion. 2. Execute the step 1 to delete other subscribers: > One subscriber in the active state.
Expected output	# The "Subscriber list" window is active without the deleted subscriber. # The subscriber in the active state is not deleted. # The subscriber, which belongs to several groups, is deleted.
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ***Anomaly Sheet Ref :*** ☐ **Not Blocking**

6.4 Notification Message Tests

The product must manage some pre or/and post notification messages to inform the subscriber of the provisioning transaction execution (start and result).

These different messages are managed by the platform in the "notification message management". Also the platform provides to the end user some error messages in case of problems during the provisioning transaction:

- Pre notification messages are displayed on the handset screen in case of normal execution to inform the subscriber on the future provisioning.
- Error messages are displayed in case of error to notify him that the provisioning transaction can not be performed due to an indicated reason.
- Post notification messages are displayed to inform the subscriber that the service had been safely provisioned on his handset.

A notification message is defined by a name, a wording, a state (active or inactive) and a type (pre, post-notification or error message). The delays between the pre notification and the provisioning or between the provisioning anf the post-notification message are defined in the GemConnect Device Manager product parameters.

Only an administrator can do the corresponding actions done on the notification message management. The customer care can only search the different notification messages. The subscriber has no access to this functionality.

6.4.1 Notification Creation

This procedure needs a message name, a type (PRE, POST, ERROR) and a message wording.

This provisioning will be tested on the handset during the provisioning transaction part of the product acceptance.

Each notification message creation generates an XML file under the folder defined by the GDM parameter "GENERAL - NOTIFICATION_MESSAGE".

Function verified	**Creation of new notification message by using the CCI**
Pre requisites	Access to the OTA Manager GUI. The profile used for the execution is an administrator profile with the "Setting Set Management" and the "Setting Set Viewing" access rights.
Test directions	1. Notification Creation: > Select the item "Notification Management" and then "Notification / Create". > Fulfil all fields for the notification message AccPreMessage00: _ Current Status: Active. _ Type: Pre-notification. _ Message: AccPreMessage00 pre-notification message. > Click on the "Create" Button 2. Notification Viewing: > Click on the "View" button. > Visualise and check the different properties of the message definition. > Click on the "Show linked devices and services" button. > Click on the "Back" button to come back to the message notification properties. > Click on the "Back" button to come back to the message list.
Expected output	*# The "Notification message search" window is active with the AccPreMessage00 in the label field.* # The different properties displayed in the notification properties correspond to those inserted in the previous steps. # At that time, there is no link to services and/or devices for this new message.

21/12/2010

Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ☐ **Not Blocking** ***Anomaly Sheet Ref :***

6.4.2 Notification Deletion

The deletion is possible even if the notification message is used by a service. The deletion is possible only if the notification is in the inactive state. At the message deletion, the corresponding XML file.

Function verified	**Notification message deletion on the product through Device Manager CCI**
Pre requisites	Access to the OTA Manager GUI. The profile used for the execution is an administrator profile with the "Setting Set Management" and the "Setting Set Viewing" access rights. Some notification messages must be already provided in the platform. Some of them must be used by a services and the other must be free. Some of them must be activated and the other must be deactivated.
Test directions	1. Notification Deletion: > Select the item "Notification Management" and then "Notification / Search For". > Select a type in the Type list. > Click on the "Search" button to launch the research. > Select in the messages list an inactive notification. > Click on the "Delete" button to delete the selected notification. > Click on the "Cancel" button to cancel the action. > Click on the "Delete" button to delete the selected notifications. > Click on the "OK" button to confirm the deletion. 2. Execute the step 1 to delete other notification messages: > One is activated. > One is deactivated but used by several services and handsets. 3. Execute the step 1 after the deletion of the different links dealing with the selected notification message.
Expected output	# The message is deleted from the list. # The active notification message is not deleted with a error message. *# The deactivated notification message used by services and handsets is deleted safely without any error message.*
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ☐ **Not Blocking** ***Anomaly Sheet Ref :***

6.4.3 Notification Link Management

The procedures dedicated to the device capabilities batch loading deal with the link management.

But this procedure checks the creation and the modification by using the GUI.

21/12/2010

It is important to understand that the LinqUS Device Manager product creates only links compliant with the handset capabilities. If for a specific handset, all services are selected in the link creation window, the product will create only the links to services available on the corresponding handset according to its capabilities.

Function verified	**Notification message link management through Device Manager CCI**
Pre requisites	Access to the OTA Manager GUI. The profile used for the execution is an administrator profile with the "Setting Set Management" and the "Setting Set Viewing" access rights. Some notification messages must be already provided in the platform. Some handsets must be already provided in the platform.
Test directions	1. Notification Link creation: > Select the item "Notification Management" and then "Notification/ Search For". > Select a type in the type list. > Click on the "Search" button to launch the research. > Select in the messages list a notification message "AccPreMessage00". > Click on the "Link to device" button. > Fulfil in the "Device dependencies" and "Service dependencies" window some fields to select some devices and some services to the message. > Click on the "Link to device" button. 2. Notification Link viewing: > Click on the "View" button. > Visualise and check the different properties of the notification description. > Click on the "Show linked devices and services" > Visualise and check the links with services and devices. > Click twice on the "Back" button to come back to the message list. 3. Notification Link modification: > Select the item "Notification Management" and then "Notification/ Search For". > Select a type in the type list. > Click on the "Search" button to launch the research. > Select in the messages list the previous notification message. > Click on the "Link to device" button. > Fulfil in the "Device dependencies" and "Service dependencies" window some fields to select some devices and some services to the message. > Click on the "Link to device" button. 4. Notification Link viewing: > Click on the "View" button. > Visualise and check the different properties of the notification description. > Click on the "Show linked devices and services" > Visualise and check the links with services and devices. > Click twice on the "Back" button to come back to the message list. 5. Notification Link deletion: > Select the item "Notification Management" and then "Notification/ Search For". > Select a type in the type list. > Click on the "Search" button to launch the research. > Select in the messages list the previous notification message. > Click on the "Delete link to device" button. > Select one or several (using the CTRL or MAJ keys) links to delete for the selected notification message. > Click on the "Delete" button.

21/12/2010

	> Click on the "Back" button to come back to the notification message list. 6. Notification Link viewing: > Click on the "View" button. > Visualise and check the different properties of the notification description. > Click on the "Show linked devices and services" > Visualise and check the links with services and devices. > Click twice on the "Back" button to come back to the message list.
Expected output	# The "Message list" window is active with the modified notification in the label field. # The links with devices and services must be in accordance with those defined during the previous step and the handset capabilities. # The previous links do not appear in the link window. # The "Message list" window is active with the modified notification in the label field. # The links with devices and services must be in accordance with those defined during the 2 previous steps and the handset capabilities. # The links are deleted from the link window. # The "Message list" window is active with the modified notification in the label field. # The links with devices and services must be in accordance with those defined and deleted during the 3 previous steps and the handset capabilities.
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ☐ **Not Blocking** ***Anomaly Sheet Ref :***

6.5 Provisioning Transaction Management Tests

The provisioning transaction aims at sending to the handset the settings for a specific service. A provisioning transaction is constituted by a target (MSISDN) and a service to provision on its device. During the provisioning transaction, the platform user has to define some parameters specific to the targeted subscriber.

These tests are executed in a real environment with a product connected to a SMSC and with one or several handsets embedded a SIM card.

This action can be done by an administrator for test, by a customer care on the telecom operator subscriber and the subscriber only on his own device.

6.5.1 Service List according to handset capabilities

This procedure is executed with MSISDNs linked to different handset types. It checks in the same time the fields fulfilled by specific subscriber data. This test is an end to end test with a real environment.

Function verified	**Available services for an msisdn is in accordance to its handset capabilities**
Pre requisites	Access to the OTA Manager GUI. The product is integrated to a real environment with an SMSC connection, a mobile and an SIM card. Several handsets must be already provisioned in the platform. Several subscriber handsets must be already provisioned in the platform.
Test directions	1. Subscriber selection:

	> Select the item "Transaction Management" and then "Transaction / Submission". > Insert the MSISDN value of an existing subscriber. > Click on the "Search" button. > Select one setting sets in the setting set list. 2. Setting set selection: > Select one setting sets in the setting set list. 3. Transaction submission: > Click on the "Submit" button to execute the provisioning transaction. > Fulfil the relevant subscriber-dependent parameters with values. 4. Transaction monitoring: > Select the item "Transaction Management" and then "Transaction / Monitoring". > Click on the "View" button. > Click on the "Refresh" button to see the request execution. 5. Handset checking: > Verify on the handset that the setting sets has been received and working fine.
Expected output	# The current handset and the list of the subscribed service appear in the window. # The handset references must be equal to the current device of the subscriber. *# The subscribed service list must contain only the services available for the current subscriber and its handset.* *# The subscriber-dependent parameters not relevant for the selected service are fulfilled with "NOT APPLICABLE".* *# A message appears to specify that the request is submitted to the platform.* # The different provisioning transactions in process or executed appear in the list. *# The transaction submitted in the previous step must appear with a state and an ending status.* *# The different parameter values must be in accordance with those provisioned during the provisioning transaction.*
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ☐ **Not Blocking** ***Anomaly Sheet Ref :***

6.5.2 Provisioning Transaction Monitoring

This procedure aims at checking the provisioning transaction monitoring with the different states and ending status. In the same time, the actions available in the monitoring are verified.

Function verified	**Monitoring of provisioning transactions**
Pre requisites	Access to the OTA Manager GUI. The product is integrated to a real environment with an SMSC connection, a mobile and an SIM card. Several handsets must be already provisioned in the platform. Several subscriber handsets must be already provisioned in the platform.
Test directions	1. Subscriber selection: > Select the item "Transaction Management" and then "Submission". > Insert the MSISDN value of an existing subscriber. > Click on the "Search" button.

21/12/2010

2. Service selection:
   > Select in the subscribed service list one available service.
   > Select the different setting sets.

3. Setting set selection:
   > Select one setting sets in the setting set list.
   > Fulfil the relevant subscriber-dependent parameters with values.

4. Transaction submission:
   > Click on the "Submit" button to execute the provisioning transaction.

5. Transaction deleting:
   > Select the item "Transaction Management" and then "Monitoring".
   > Click on the "View" button.
   > Select the last provisioning transaction.
   > Click on the "Delete" button to suppress the execution.

6. Handset checking:
   > Verify, if it is possible, on the handset that the setting sets is not downloaded safely.

7. Transaction replay:
   > Select the last provisioning transaction which was deleted.
   > Click on the "Replay" button to replay the request.

8. Handset checking:
   > Verify, if it is possible, on the handset that the setting sets is downloaded safely.

9. Platform checking:
   > Select the item "Subscriber Management" and then "Subscriber / Search For"
   > Create in the "Subscriber search" window a request to select the target of the previous provisioning transaction.
   > Click on the "Search" button to launch the research.
   > Select in the subscriber list the subscriber.
   > Click on the "View" button.
   > Click on the "See Configuration" button of the service selected for the provisioning transaction.
   > Select the setting set used in the previous provisioning transaction.

10. Transaction acknowledge:
    > Select the item "Transaction Management" and then "Monitoring".
    > Click on the "View" button.
    > Select a provisioning transaction with the state "Terminated".
    > Click on the "Acknowledge" button to acknowledge the transaction result.

11. Other transaction acknowledges:
    > Select several provisioning transactions with a state "Terminated".
    > Click on the "Acknowledge" button to acknowledge the transaction results.

21/12/2010

	> Select a provisioning transaction with a state different from "Terminated". > Click on the "Acknowledge" button to acknowledge the transaction results. 12. Other transaction acknowledges: > Select all the provisioning transactions in the monitoring by clicking on the "Select all" button. > Deactivate the selection of the different transaction with a state different from "Terminated". > Click on the "Acknowledge" button to acknowledge the transaction results.
Expected output	# The current handset and the list of the subscribed service appear in the window. # The handset references must be equal to the current device of the subscriber. *# The subscribed service list must contain only the services available for the current subscriber and its handset.* # All setting sets available for this service appear in the setting set list. # For only one setting set, it is possible that the "Configured" checkbox is activated. In this case, this activation must be in accordance with the subscriber properties. # For only one setting set, it is possible that the "Default" checkbox is activated. In this case, this activation must be in accordance with the subscriber properties. *# For one or several setting set, it is also possible to have some subscriber-dependant parameters fulfilled. In this case, these parameters must be in accordance with the subscriber properties.* *# The subscriber-dependent parameters not relevant for the selected service are fulfilled with "NOT APPLICABLE".* *# A message appears to specify that the request is submitted to the platform.* # The different provisioning transactions in process or executed appear in the list. # The transaction execution is stopped. The handset does not receive all SMS for the provisioning. *# The state of the request is "Terminated" and the ending status is "Deleted".* *# The setting set is not present on the handset.* # The different provisioning transactions in process or executed appear in the list. # A new transaction is added to the list with the state "In process". # The transaction submitted in the previous step must appear with a state and an ending status. *# The state of the request is "Terminated" and the ending status is "Deleted".* *# The different parameter values must be in accordance with those provisioned during the provisioning transaction.* # The subscriber-dependent parameters are fulfilled with the values inserted during the provisioning transaction. *# The "Configured" checkbox is activated.* # The different provisioning transactions in process or executed appear in the list. *# The selected provisioning transaction is deleted from the list.* # The different provisioning transactions in process or executed appear in the list. # The selected provisioning transactions with the "Terminated" state are deleted from the list. *# For the provisioning transactions with another states, an error message appears to warn that the acknowledgement is not possible for this state.* # The different provisioning transactions in process or executed appear in the list. *# The selected provisioning transactions with the "Terminated" state are deleted from the list.*
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ☐ **Not Blocking** ***Anomaly Sheet Ref :***

6.5.3 Provisioning Transaction Search

In the provisioning transaction monitoring, it is possible to search different transactions according to:

- Their current state
- Their ending status
- Criteria defined in the GUI

In the same time, the results can be sorted according to different properties like the submission date or the requested service.

Function verified	**Provisioning transaction search tool on Device Manager CCI**
Pre requisites	Access to the OTA Manager GUI. The product is integrated to a real environment with an SMSC connection, a mobile and an SIM card. Several handsets must be already provisioned in the platform. Several subscriber handsets must be already provisioned in the platform. This procedure must be executed after several tests on the provisioning transaction.
Test directions	1. Transaction search: > Select the item "Transaction Management" and then "Monitoring". > Select some states and ending status. > Insert some criteria to sort the results. > Click on the "View" button. 2. Transaction checking: > Click on the "Information" button of several provisioning transactions in the monitoring. 3. Transaction search: > Select the item "Transaction Management" and then "Monitoring". > Select some states and ending status. > Insert some criteria to sort the results. > Insert some criteria to select the provisioning transactions. These criteria must be in accordance with the transactions already present in the monitoring. > Click on the "View" button. 4. Transaction checking: > Click on the "Information" button of several provisioning transactions in the monitoring.
Expected output	# The list of the provisioning transactions appears. # The list must contain the transactions in accordance with the chosen states and ending status. *# The list must be sorted according to the criteria defined in the research.* *# The transaction properties must be in accordance with the search and sorting criteria.* # The list of the provisioning transactions appears. # The list must contain the transactions in accordance with the chosen states, ending

21/12/2010

	status and the other criteria. *# The list must be sorted according to the criteria defined in the research.* *# The transaction properties must be in accordance with the search and sorting criteria.*
Noted output	
☑ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ***Anomaly Sheet Ref :*** ☐ **Not Blocking**

6.6 Device Detection Tests

6.6.1 IMEI change detection and storing

Function verified	**When a new IMEI is received Device Detection stores it in the database**
Pre requisites	Access to the OTA Manager GUI. Device Manager must be configured to work with the Device Detection module. Device Detection applet must be installed in the SIM Cards to be used for the test. Two handsets required for this test: #1 and #2.
Test directions	1. IMEI sending and storing: > Insert the SIM Card in the handset #1 and turn it on. 2. IMEI sending and updating: > Remove the SIM Card from the handset #1 and place it in the handset #2. Turn it on.
Expected output	# A SMS MO is received in the IMEI tracking module # In the IMEI database the MSISDN of the testing simcard is associated to the IMEI of the handset #1. # A SMS MO is received in the IMEI tracking module # In the IMEI database the MSISDN of the testing simcard is associated to the IMEI of the handset #2.
Noted output	
☐ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ***Anomaly Sheet Ref :*** ☐ **Not Blocking**

6.6.2 Automatic Provisioning

Function verified	**Device Manager sends the configuration parameters to the new handset after the SIM Card has been changed from one handset to a new one**
Pre requisites	Access to the OTA Manager GUI. Device Manager must be configured to work with the Device Detection module. Device Detection applet must be installed in the SIM Cards to be used for the test. Two handsets required for this test: #1 and #2.
Test directions	1. New IMEI sending: > Move the SIM Card from handset #2 to handset #1. Turn it on.

Expected output	# A SMS MO is received in the IMEI tracking module # In the IMEI database the MSISDN of the testing simcard is associated to the IMEI of the handset #1. # The GDM detects a change of handset and sends the configuration of the new handset (#1). # The handset receives the configuration and updates the parameters.
Noted output	
☐ **Compliant** ☐ **Blocking**	☐ **Not Compliant** ***Anomaly Sheet Ref :*** ☐ **Not Blocking**

7 Acceptance Acknowledgement

Signing below states the approval of the deliverables and, in case of approval, acknowledges that the deliverables conform to the LinqUs Device Manager solution. To the extent of conflicting acceptance terms between this Customer Acceptance and the Purchase Order, this Customer Acceptance shall be deemed an amendment of the Purchase Order.

Por Ericsson/ICE Costa Rica	**Por Gemalto**
Nombre: MacSee Vallejos	Nombre: Rodrigo Pliego Sánchez
Puesto: Managed Service Technician	Puesto: Ingeniero Integrador
Fecha: Martes, 21 de Diciembre de 2010	Fecha: Martes, 21 de Diciembre de 2010
Firma:	Firma:
Nombre: Pablo Murillo	Nombre: Miguel Serrano
Puesto: Project Manager	Puesto: Gerente de Proyecto
Fecha: Martes, 21 de Diciembre de 2010	Fecha: Martes, 21 de Diciembre de 2010
Firma:	Firma:

☐ Compliant	☐ Not compliant	Anomaly reference:

Remarks:

8 Annex1: Anomaly Sheet

OPERATOR **LinqUs Device Manager** **Integration Anomaly Sheet**	**Anomaly Ref:** **Date (dd/mm/yyyy):** / /

Nature:	**Type:**	**Class:**
❑ Software ❑ Documentation ❑ Else	❑ Severe ❑ Minor	❑ Default ❑ No conformity ❑ Undefined

Test reference:

Description:

Fixed by:
Date:
Fix Description:

Verified by:
Date:

- END OF DOCUMENT -