Cellact Large Account v.3.2 HTTP

Interface Description

Important Notice

Contents

List of Tables

1. Preface

1.1 Purpose and Scope

This document describes the Cellact Large Account (LA) HTTP interface and XML configuration. The Large Account application platform provides enterprises and content providers with the ability to send and receive SMS and MMS messages to and from mobile operators, in Israel or abroad.

The guide includes the following main topics:

Large Account Overview

Protocol Description

Commands

Mobile Originated Message

Reverse Billing Model

MO/MT Model

MOMMS Model

The appendices include:

Code Example

Acronyms

1.2 Audience

This guide is intended for the mobile provider's system operators. It is assumed that users of the interface are familiar with Cellact Large Account systems and with XML.

2. Large Account Overview

The Large Account (LA) application platform provides enterprises and content providers with the ability to send and receive SMS and MMS messages to and from mobile operators, in Israel or abroad.

The LA provides several types of interfaces including HTTP/XML, Web service, SMTP and SMPP.

The scope of this document explains the use of the HTTP based interface.

2.1 System Architecture
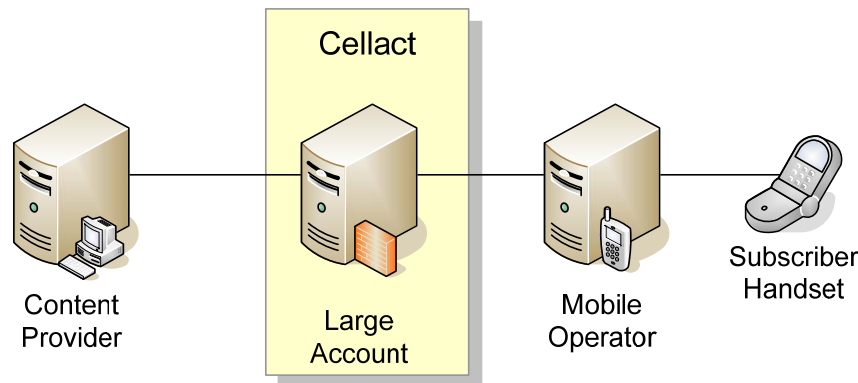
Figure 1: Large Account System Architecture

2.2 Requirements

The following are the basic requirements for sending SMS messages using the Large Account application.

You should ensure that the following actions are performed on the client side:

■ Open a Large Account on the HTTP Large Account (LA) application.

■ Provide a well-known legal IP address on the Internet from where the HTTP/POST requests can be sent to the Large Account application.

NOTE

When the Large Account server receives a message from the client, it checks if there is a match between the message's IP address and the address of the company that sent the message.

■ Assign a unique enterprise name identifier as registered with the LA application.

■ Assign a user name and password to the LA application.

■ Connect to the Internet.

■ Check if the connection to the Internet is established via a TCP/IP port 80 or via the HTTP protocol (firewall rules).

3.   Protocol Description

3.1   XML Structure and Parameters

The LA HTTP/XML protocol requires a HTTP post request with a specific XML format in order to send a message. The message uses the POST method with a single parameter named: "XMLString".

The XMLString parameter contains the XML string that is used in the request.

The XML structure is described for each command. This format includes a HEAD section for general information on the message including authentication fields, as well as a BODY section that provides the specific data of the command. There is also the OPTIONAL section that contains optional parameters.

Table 1 lists the parameters are used in the XML:

Table 1: XML Parameters

Field	Description
APP	The application that generated the message. **Note**: APP must always be a fixed value string– 'LA' (Large Account).
BODY	Contains command-related data, such as sender, message content and destination numbers.
CMD	Any messaging command or command alias.
FROM	Enterprise unique name (provided by Cellact).
HEAD	Message-related data.
MSG_ID	Optional. A unique identifier provided by the client to sign its messages.
OPTIONAL	Client-side tags that are allowed but optional.
PALO	The root tag of the XML request.
TTL	Optional. Time To Live. Used to set the message expiry date. The period of time that the operator's SMSC retains a message in case of delivery failure before the message is expired. The default limit is 1440 minutes (1 day). The minimum limit is 15 minutes.
TTS	Optional. Time To Schedule. Used to sending a scheduled message, that is to allow messages to be sent up to a number of days. The maximum limit is 10080 minutes (7 days) from the current/schedule date.
USER & PASSWORD	User and password of the LA as provided by Cellact.

3.1.1 Example: Sending by POST Method

Let's start by looking at a simple example of how to send a POST request:

```
<PALO>
    <HEAD>

        <FROM>Company_name</FROM>

        <APP USER="username" PASSWORD="123456">LA</APP>

        <CMD>sendtextmt</CMD>

    </HEAD>

    <BODY>

        <SENDER>+97256337000</SENDER>

        <CONTENT><![CDATA[Hello, world!]]></CONTENT>

        <DEST_LIST>

            <TO>+972506501020</TO>

        </DEST_LIST>

    </BODY>

    <OPTIONAL>

        <MSG_ID>1123527</MSG_ID>

    </OPTIONAL>

</PALO>
```

This is the XML that is sent as a parameter in the HTTP/POST request.

This means that the content of the POST request looks like this:
XMLString=<PALO><HEAD>….</PALO>

Pay attention to the following issues:

- **URL Encoding:** You should always use URL encoding to ensure that characters are encoded correctly, for example when applying to a URL. Every space in the text is replaced with the characters: %20 (spaces are not allowed). The same applies to special characters such as signs: '<' or '>'.

- **Unicode**: The XML format should be in UTF-8 – Unicode. This allows supporting a set of languages, including Hebrew.

- **Destination Number**: The destination number may contain an international dialing format in order to support target numbers abroad.

- The Large Account URL address is: http://la.cellactpro.com/unistart5.asp

The following example includes the TTL and TTS optional tags.

```
<PALO>

    <HEAD>

        <FROM>company name</FROM>

        <APP USER="user name" PASSWORD="password">LA</APP>

        <CMD>sendtextmt</CMD>

        <TTL>180</TTL>

        <TTS>90</TTS>

    </HEAD>

    <BODY>

        <SENDER>+97256337000</SENDER>

        <CONTENT>Test TTL and TTS options</CONTENT>

        <DEST_LIST>

            <TO>+972506501020</TO>

        </DEST_LIST>

    </BODY>

</PALO>
```

3.1.2 Example: Sending by GET Method

Let's start by looking at a simple example of how to send a GET request. The following link includes the GET parameters:

http://la.cellactpro.com/http_req.asp?FROM=CompanyName&USER=username&PASSWORD=password&APP=LA&CMD=sendtextmt&SENDER=6655&CONTENT=Test the GET method&TO=0501234567&SN=SMS&MSGID=123456&CONFMAIL=Example@test.com

You should change the parameter values that are indicated in red, and then use the link to send a message.

Table 2 lists the parameters are used by the GET method SMS:

Table 2: GET Request Parameters

Field	Description
FROM	Enterprise name (provided by Cellact).
APP	The application that generated the message. **Note**: APP must always be a fixed string value – 'LA' (Large Account).
USER	A unique user name for the Enterprise (provided by Cellact)
PASSWORD	A unique user password (provided by Cellact).
CMD	A command for sending a message (sendtextmt).
SENDER	The sender's mobile phone number.
CONTENT	The text of the message that will be displayed on subscriber handset. **Note**: Hebrew content must be coded to Unicode. Example: %u05D0%u05D1%u05D2 (אבג)
TO	The destination mobile phone number, in local or international format. **Note**: Up to 20 numbers can be placed in a request.
SN	Optional. Service Name – the name of the service application that is being used, for client support purposes.
MSGID	Optional. A unique identifier provided by the client to sign its messages.
CONFMAIL	Optional. The email address to which the confirmation of service will be sent.

NOTE

The GET Method does not support with TTL TTS options.

3.2   Response Message Format

The Large Account gateway returns a HTTP 200 Ok in response to a request and provides an XML with success or failure indication.

Response to Successful

Here is an example of an XML response to a successful request:

```
<PALO>
    <RESULT>True</RESULT>
    <SESSION>4e07d3be-eb3f-4d98-ace6-fd90342b0dec</SESSION>
    <OPTIONAL>
        <MSG_ID>12345</MSG_ID>
        <SERVICE_NAME>SMS</SERVICE_NAME>
    </OPTIONAL>
</PALO>
```

The SESSION tag indicates a unique request identifier that shall be used for further notifications on the message result.

Response to Failed

Here is an example of an XML response to a failed request:

```
<PALO>
    <RESULT>false</RESULT>
    <DESCRIPTION>not an authorized user</DESCRIPTION>
    <OPTIONAL>
        <MSG_ID>1123528</MSG_ID>
    </OPTIONAL>
</PALO>
```

The OPTIONAL tag that was provided in the request is also returned by the Large Account gateway in its response. The same tag is also used in the confirmation of delivery mechanism, as described in Confirmation on Delivery.

3.3   Required Account Details and Verification

When Cellact opens a new account for you, you should ensure that you have the following information:

■ **Account**: A new account is opened for you on the Cellact Large Account gateway. Cellact provides the FROM, USER and PASSWORD data necessary for account authentication.

■ **IP address**: A valid and well-known IP address of the account, from which the HTTP/POST requests shall be sent via Internet to the Large Account gateway.

This address must be provided to Cellact support personnel.
For contact with Cellact, call us or write to support@cellact.com.

When the Large Account server receives a message from a client, it verifies if there is a match between the message's IP address and that of the company that sent the message. The parameters used for matching are:

■ **Unique enterprise name identifier** as registered with the LA application. This is the FROM tag.

■ **User and password** of the Large Account.

■ Cellact also requires **connectivity** to the Internet via port 80 with HTTP protocol or port 443 using HTTPS.

While the system accepts requests that are in other formats, they are rejected before they reach the SMSC of the mobile operator, and are not delivered.

The sender's phone number (Call back number) may be any valid telephone number or short number (for example +972506123456 or 1234). This number appears in the Reply field on the target device.

3.4   Authentication Mechanism

The Authentication mechanism identifies the incoming requests. Authentication is based on the following parameters:

- ■ FROM tag (the company name)
- ■ Username attribute
- ■ Password attribute
- ■ IP address

NOTE

The incoming requests should always have a fixed IP address.

3.5   Billing Models

The following types of billing model are available:

- ■ **Regular message**: The content provider is charged for every message it sends. This is the regular message model.

- ■ **Reverse Billing message**: Reverse Billing. Premium charge – the subscriber that receives the message is charged.

  For more information, see Reverse Billing Model.

- ■ **MO/MT model**: Transaction model – a Mobile Originated (MO) message that is routed to a content provider must be answered within 12 seconds with a Mobile Terminated (MT) message in order to close the transaction. The limitation of 12 seconds applies only to the Orange network.

  For more information, see Mobile Originated Message and MO/MT Model.

- ■ **MOMMS model**: This mobile originated messaging model allows the content provider (CP) to receive rich content such as pictures, movies and recordings in image, video, or audio files using either email or an MO SMS message.

  For more information, see MOMMS Model.

NOTE

- ● **In the Orange network, there is no option to use Reverse Billing messages for prepaid subscribers.**

- ● **In the MO/MT model on the Orange network, it is important to return the MT message within 12 seconds. In case the transaction is not closed in time, the subscriber receives a notification that the message was not delivered and therefore was not charged.**

- ● **In the Mirs network, it is not possible to set the Sender field; it is replaced with a fixed number that is used for billing purposes.**

3.6 Message Length Limitations

Operator support for SMS varies, depending on the maximum allowed message length and on message concatenation support. These two factors influence the SMS setup and display, as well as billing.

Operators use two methods to process messages that exceed the preset text limit:

■ **Concatenation**: Concatenation is a system feature that allows for dividing and sending a longer SMS so it is displayed as two or three pages on the handset screen. Concatenated messages are charged according to message length.

■ **Splitting**: Operators who do not support concatenation use the split method where messages longer than the set limit arrive at the subscriber's handset as separate messages, not as a single 2-3-page concatenated message. The split messages are charged independently.

NOTE

Message that contains one or more non-Latin characters is billed and considered as a Unicode message.

Table 3 lists the concatenation support and the supported maximum message length per operator in characters for each type of interface (Unicode or English).

Table 3: Message Length Limit per Operator

Operator	Concatenation Support	Unicode (non-Latin, incl. Hebrew, mixed)		English (Latin chars only)	
		Single	Concat.	Single	Concat.
Cellcom	Yes	70	800	160	800
Mirs	No – (split)	70	132	160	-
Orange	Yes	70	800	160	800
Pelephone	No – CDMA (split)	70	800	160	800
Pelephone	Yes – UMTS	70	800	160	800
Home Cellolar	Yes	70	800	160	800
Rami Levi	Yes	70	800	160	800
Golan Telecom	Yes	70	800	160	800
Hot Mobile	Yes	70	800	160	800

Outside Israel (GSM networks)	No	70 characters	800	160	800

3.7   Mobile Number Portability (MNP)

Mobile number portability enables the mobile subscriber to move from one network to another while retaining the same phone number.

For example, a Pelephone subscriber number 050-6501020 that moves to the Cellcom network keeps the same number 050-6501020. This means that there is no more option to identify the network according to the operator prefix – so we have to query an updated database for the location of the mobile subscriber.

What is the impact of this feature?

A content provider that intends to deliver specific content aimed at a specific network should know beforehand if the target subscriber belongs to that network. The content provider should also be aware of the message limitations valid in the subscribers' network.

In order to find out which network the subscriber belongs to, you may use the following options:

■ Send a message to Cellact, and we shall route the message to the correct network.

■ Send a Query MNP HTTP request to Cellact for the subscriber's number, and get a response notification that includes the operator prefix, for example
```
<RECIPIENT MNP="97250">+972501234567</RECIPIENT>.
```

■ Use the MO/MT Model. In the MO/MT model, the subscriber network is indicated in the MO message.

3.7.1 Query MNP

When querying the MNP if a mobile subscriber belongs to another network (according to the operator's prefix), apply the following default URL: http://la.cellactpro.com/mnp.asp

The HTTP/POST XML request is the same as any other Large Account request. Entering the <CMD>**mnp**</CMD> command in the CMD tag in the HEAD section and the subscribers on the DEST_LIST.

Here is an example of the complete request and BODY section for this command:

```
<PALO>

    <HEAD>

        <FROM>Company_name</FROM>

        <APP USER="username" PASSWORD="123456">LA</APP>

        <CMD>mnp</CMD>

    </HEAD>

    <BODY>

        <DEST_LIST>

            <TO>+972506501020</TO>

        </DEST_LIST>

    </BODY>

</PALO>
```

The response shall include the OP attribute that indicates the network/operator that the subscriber belongs to:

```
<PALO>

    <RESULT>true</RESULT>

    <DEST_LIST>

            <TO OP="97252">+972506501020</TO>

    </DEST_LIST>

</PALO>
```

3.7.2   OP Numbers

Table 4 lists the operators' OP numbers:

Table 4: OP Numbers

Operator	OP Number
Cellcom	97252
Mirs	97257
Orange	97254
Pelephone	97250
Bezeq	9723
Home Cellolar	9725522/23
Rami Levi	9725566/67
Golan Telecom	97258
Hot Mobile	97253

NOTE

Currently, the DEST_LIST in an MNP query message may contain only one OP number. Future LA versions may provide the option to query more numbers.

3.7.3   Exceeded Throttling Limit Error

The Query MNP interface is limited by the throttling value that is set per account. This means that each account is provisioned to process up to a certain number of messages per second.

An account that exceeds the throttling limit that the system set for it, shall receive a negative acknowledgment with an appropriate error description.

For example:

```
<PALO>
    <RESULT>false</RESULT>
    <DESCRIPTION>throttle error</DESCRIPTION>
</PALO>
```

4. Commands

The following message commands are available in the LA HTTP interface v.3.2:

Sendtextmt   Send a mobile terminated SMS message.

Sendlinkmt   Send a mobile terminated WAP link message.

Sendwaptextmt   Send a mobile terminated WAP link message with a
                        response option.

Sendringtonemt   Send a mobile terminated binary ringtone message.

Sendoperatorlogomt   Send a mobile terminated operator logo message.

Sendpicturemt   Send a mobile terminated picture message.

Sendmms   Send a mobile terminated MMS message.

NOTE

**The sendiconmt command that was included in previous versions of this
guide is being phased out and has been removed from the list.**

4.1   Sendtextmt

NOTE

The request's DEST_LIST may contain up to 200 destination numbers.

Entering the <CMD>**sendtextmt**</CMD> command in the CMD tag of the HEAD section sends a text message to the list of subscribers on the DEST_LIST.

Here is an example of the complete request and BODY section:

```
<PALO>

    <HEAD>

        <FROM>Cellact</FROM>

        <APP USER="username" PASSWORD="123456">LA</APP>

        <CMD>sendtextmt</CMD>

    </HEAD>

    <BODY>

        <SENDER>+972506337000</SENDER>

        <CONTENT>Hello, world!</CONTENT>

        <DEST_LIST>

            <TO>+972506501020</TO>

        </DEST_LIST>

    </BODY>

    <OPTIONAL>

        <MSG_ID>1123528</MSG_ID>

    </OPTIONAL>

</PALO>
```

4.2   Sendlinkmt

NOTE

The following limitations apply to sendlinkmt requests:

● **The length of the link name and the URL (assuming use of Latin characters only, such as English) may contain up to 160 characters.**

● **The request's DEST_LIST may contain up to 200 destination numbers.**

● **The Content may contain up to 40 characters.**

Entering the <CMD>**sendlinkmt**</CMD> command in the CMD tag of the HEAD section sends a URL link message (usually used for WAP links) to the list of subscribers on the DEST_LIST.

The CONTENT tag (up to 40 characters) provides the title that shall appear in the link.

The LINK tag is the URL used by the client for connecting to the Web site provided in the URL link message.

Here is an example of the complete request and BODY section for this command:

```
<PALO>

    <HEAD>

        <FROM>Company_name</FROM>

        <APP USER="username" PASSWORD="123456">LA</APP>

        <CMD>sendlinkmt</CMD>

    </HEAD>

    <BODY>

        <SENDER>+972506337000</SENDER>

        <CONTENT>Hello, world!</CONTENT>

        <LINK>http//www.cellact.com/MyWapPage.wml</LINK>

        <DEST_LIST>

            <TO>+972506501020</TO>

        </DEST_LIST>

    </BODY>

    <OPTIONAL>

        <MSG_ID>1123528</MSG_ID>

    </OPTIONAL>

</PALO>
```

4.3   Sendwaptextmt

The following limitations apply to sendwaptextmt requests:

- **The length of the link name and the URL (assuming use of Latin characters only, such as English) may contain up to 160 characters.**
- **The request's DEST_LIST may contain up to 200 destination numbers.**
- **The Content may contain up to 40 characters.**

Entering the <CMD>**sendwaptextmt**</CMD> command in the CMD tag of the HEAD section sends a WAP message to the list of subscribers on the DEST_LIST.

The CONTENT tag (up to 40 characters) provides the title that shall appear in the link.

The **Title** tag provides the title that appears on the message at arrival.

To receive a reply from the customer, to the address defined in the CONF_LIST, add a **Template** tag with the word **reply** in it.

Here is an example of the complete request and BODY section for this command:

```
<PALO>

    <HEAD>

        <FROM>Company_name</FROM>

        <APP USER="username"  PASSWORD="123456">LA</APP>

        <CMD>sendwaptextmt</CMD>

        <CONF_LIST><TO
TECH="post">http://hello.com/cod.asp</TO></CONF_LIST>

    </HEAD>

    <BODY>

    <SENDER>+972506337000</SENDER>

    <CONTENT> Hello, world!</CONTENT>

        <DEST_LIST>

            <TO>+972506501020</TO>

        </DEST_LIST>

    </BODY>

    <OPTIONAL>

<WAP>

    <Title>my title</Title>

        <Template>reply</Template>

    </WAP></OPTIONAL></PALO>
```

4.3.1   Subscriber response

The **sendwaptextmt** command enable to receive the subscriber respond via XML to the specify URL inserted in <CONF_LIST> tag**.**

Here is an example of a response that can arrive from the subscriber:

```
CONFIRMATION=

<PALO>

    <BLMJ>37f289e3-dca5-436a-8ddc-28257507d48a</BLMJ>

    <SENDER>1234</SENDER>

    <RECIPIENT MNP="">+972501234567</RECIPIENT>

    <FINAL_DATE>20080803122112</FINAL_DATE>

    <EVT>mt_reply</EVT>

    <REASON>7000</REASON>

    <REPLY>WAP test successful</REPLY>

    <MESSAGE_COUNT>1</MESSAGE_COUNT>

</PALO>
```

4.4   Sendringtonemt

NOTE

- **This command is supported only for GSM networks and Nokia devices used by the Orange, Pelephone and Cellcom networks.**
- **The request's DEST_LIST may contain up to 200 destination numbers.**

Entering the <CMD>**sendringtonemt**</CMD> command in the CMD tag of the HEAD section sends a ring tone message to the subscribers on the DEST_LIST.

Here is an example of the complete request and BODY section for this command:

```
<PALO>

   <HEAD>

      <FROM>Company_name</FROM>

      <APP USER="username" PASSWORD="123456">LA</APP>

      <CMD>sendringtonemt</CMD>

   </HEAD>

   <BODY>

   <SENDER>+972506337000</SENDER>
   <CONTENT>024A3A51D195CDD004001B20550590610560558550548540820849900000</CONTENT>

      <DEST_LIST>

         <TO>+97256501020</TO>

      </DEST_LIST>

   </BODY>

   <OPTIONAL>

      <MSG_ID>1123528</MSG_ID>

   </OPTIONAL>

</PALO>
```

4.5   Sendoperatorlogomt

NOTE

This command is supported only for GSM networks and Nokia devices used by the Orange and Cellcom networks.

Entering the <CMD>**sendoperatorlogomt**</CMD> command in the CMD tag of the HEAD section sends an operator's logo message to the subscribers on the DEST_LIST.

Here is an example of the complete request and BODY section for this command:

```
<PALO>

   <HEAD>

      <FROM>Company_name</FROM>

      <APP USER="username" PASSWORD="123456">LA</APP>

      <CMD>sendoperatorlogomt</CMD>

   </HEAD>

   <BODY>

   <SENDER>+972506337000</SENDER>
   <CONTENT>00480E010000000000000000000000000000000000000000000
00000000000000000000000000000000000000000F000007001E3C78F00780000380
214285080FC00001C0408102040FC1C71FE7814285021CE1C73FF78142850238
71C778F7814285023FF1C77077408102047FF9C778F721428508F03DFF3FE71E
3C78F0E01CFE1FC7</CONTENT>

      <DEST_LIST>

         <TO>+972506501020</TO>

      </DEST_LIST>

   </BODY>

   <OPTIONAL>

      <MSG_ID>1123528</MSG_ID>

   </OPTIONAL>

</PALO>
```

4.6   Sendpicturemt

![NOTE]

This command is supported only for GSM networks and Nokia devices used by the Orange and Cellcom networks.

Entering the <CMD>**sendpicturemt**</CMD> command in the CMD tag of the HEAD section sends a picture message to the subscribers on the DEST_LIST.

Here is an example of the complete request and BODY section for this command:

```
<PALO>

    <HEAD>

        <FROM>Company_name</FROM>

        <APP USER="username" PASSWORD="123456">LA</APP>

        <CMD>sendpicturemt</CMD>

    </HEAD>

    <BODY>

    <SENDER>+972506337000</SENDER>
    <CONTENT>00480E0100000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000F000007001E3C78F00780000380
214285080FC00001C0408102040FC1C71FE7814285021CE1C73FF78142850238
71C778F7814285023FF1C77077408102047FF9C778F721428508F03DFF3FE71E
3C78F0E01CFE1FC7</CONTENT>

        <DEST_LIST>

            <TO>+972506501020</TO>

        </DEST_LIST>

    </BODY>

    <OPTIONAL>

        <MSG_ID>1123528</MSG_ID>

    </OPTIONAL>

</PALO>
```

4.7   Sendmms

NOTE

Each mobile operator may support a different combination of MMS file formats, see also MMS Support.

Entering the <CMD>**sendmms**</CMD> command in the CMD tag of the HEAD section sends an MMS message to the subscribers on the DEST_LIST.

Sending an MMS message includes a list of files that are sent to the mobile device, currently using a simple template of the content.

Here is an example of the complete request and BODY section for this command:

```
<PALO>

    <HEAD>

        <FROM>Company_name</FROM>

        <APP USER="username" PASSWORD="123456">LA</APP>

        <CMD>sendmms</CMD>

    </HEAD>

    <BODY>

        <CONTENT><![CDATA[My MMS]]></CONTENT>

        <LINKS>

            <LINK>http://www.cellact.com/1.gif</LINK>

            <LINK>http://www.cellact.com/madonna.mid</LINK>

            <LINK>http://www.cellact.com/text.txt</LINK>

        </LINKS>

        <SENDER>+972506337000</SENDER>

        <DEST_LIST>

            <TO>+972506501020</TO>

        </DEST_LIST>

    </BODY>

    <OPTIONAL>

        <MSG_ID>1123528</MSG_ID>

    </OPTIONAL>

</PALO>
```

4.7.1   MMS Support

MMS support by the mobile operators is as follows:

- **Pelephone** supports only a single link to MMS content.
- **Orange** requires an advance notification of combination MMS messages, and supports only some format combinations.
- **Cellcom** allows combinations of different MMS file formats without any limitations.
- **Mirs** does not support MMS.

5. Confirmation on Delivery

There is an option to request a confirmation on the status of a message, in order to know if the message has reached the subscriber's handset. The confirmation is provided as a **HTTP/GET** request from the Large Account to the URL address of the content provider.

5.1 Confirmation Request

The HTTP confirmation request is always delivered on port 80 and there is no option to receive the message on a different port.

The new field that is required is the CONF_LIST that includes a TO destination to the URL address of the server of the content provider. The CONF_LIST is part of the HEAD tag.

In order to receive a confirmation, use the following format:

```
<PALO>

    <HEAD>

        <FROM>Cellact</FROM>

        <APP USER="username" PASSWORD="123456">LA</APP>

        <CMD>sendtextmt</CMD>

        <CONF_LIST>

                <TO TECH="post">http://hello.com/cod.asp</TO>

        </CONF_LIST>

    </HEAD>

    <BODY>

        <SENDER>+972506337000</SENDER>

        <CONTENT>Hello, world!</CONTENT>

        <DEST_LIST>

            <TO>+972506501020</TO>

        </DEST_LIST>

    </BODY>

    <OPTIONAL>

        <MSG_ID>1123528</MSG_ID>

    </OPTIONAL>

</PALO>
```

In response to the HTTP request generated by the content provider, a HTTP 200 Ok answer is sent with a unique SESSION identifier. This identifier is used to provide the content provider with further information on the status of a message.

When the message arrives to a new state, a notification message is sent by HTTP/GET to the content provider according to the URL address that was provided in the request. The single parameter in the request is called "confirmation" and contains the XML string.

5.1.1 MT Event States

Table 5 lists the messaging event type indicators included in the **EVT** tag of the delivery confirmation message.

Table 5: EVT Tags

EVT	Description
mt_ok	The message has arrived to the mobile operator gateway.
mt_nok	The message did not arrive to the mobile operator gateway; message was blocked.
mt_del	The message has arrived to the mobile handset.
mt_rej	The message did not arrive to the mobile handset and will never reach it.

NOTE

The Mirs network and some international mobile operators do not support confirmation on delivery.

5.1.2 Confirmation: Message Was Delivered to GW

Here is an example of a confirmation that the message has arrived at the mobile operator's gateway (SMSC):

```
CONFIRMATION=

<PALO>

    <BLMJ>37f289e3-dca5-436a-8ddc-28257507d48a</BLMJ>

    <SENDER>1234</SENDER>

    <RECIPIENT MNP="97254">+972501234567</RECIPIENT>

    <FINAL_DATE>20080803122112</FINAL_DATE>

    <EVT>mt_ok</EVT>

    <REASON>5000</REASON>

    <MESSAGE_COUNT>1</MESSAGE_COUNT>

</PALO>
```

5.1.3 Confirmation: Message Did Not Reach GW

Here is an example of a confirmation that the message did not reach the mobile operator's gateway (SMSC or MMSC) and therefore will not reach the mobile handset:

```
CONFIRMATION=

<PALO>

    <BLMJ>d7e78097-4a7f-4893-8ab9-e47f4306fb87</BLMJ>

    <SENDER>0501234567</SENDER>

    <RECIPIENT MNP="97250">+972501234567</RECIPIENT>

    <FINAL_DATE>20080731095516</FINAL_DATE>

    <EVT>mt_nok</EVT>

    <REASON>2010</REASON>

    <MESSAGE_COUNT>1</MESSAGE_COUNT>

</PALO>
```

5.1.4 Confirmation: Message Was Delivered

Here is an example of a confirmation that the message has reached the subscriber's handset:

```
CONFIRMATION=

<PALO>

    <BLMJ>a65b9a60-c8c6-46e8-9083-2113e9e98c79</BLMJ>

    <SENDER>0501235467</SENDER>

    <RECIPIENT MNP="97250">+972507124895</RECIPIENT>

    <FINAL_DATE>20080803123145</FINAL_DATE>

    <EVT>mt_del</EVT>

    <REASON>1000</REASON>

    <MESSAGE_COUNT>1</MESSAGE_COUNT>

</PALO>
```

In addition to the mt_del confirmation, a mt_ok confirmation is received from the operator's SMSC.

5.1.5 Confirmation: Message Was Not Delivered

Here is an example of a confirmation that the message was not delivered to the subscriber's handset and will never reach the handset:

```
CONFIRMATION=

<PALO>

    <BLMJ>d7e78097-4565-4893-8ab9-e47f4306fb87</BLMJ>

    <SENDER>0501234567</SENDER>

    <RECIPIENT MNP="97250">+972501234567</RECIPIENT>

    <FINAL_DATE>20080731095516</FINAL_DATE>

    <EVT>mt_rej</EVT>

    <REASON>2010</REASON>

    <MESSAGE_COUNT>1</MESSAGE_COUNT>

</PALO>
```

In addition to the mt_rej confirmation, a mt_ok confirmation is received from the operator's SMSC.

6. Mobile Originated Message

A content provider may receive mobile originated (MO) messages. A short code is routed to a URL address that is provided by the content provider. There are two ways for sending mobile originated messages: POST and GET methods. This means that every message that is generated by the subscriber and sent to a specific short code generates a **HTTP/POST** or **HTTP/GET** XML based request to the content provider.

Example of a **HTTP/POST** MO message:

```
Xml string =

<PALO>

    <HEAD>

        <BLMJ>ab259538-91b7-480d-8ae0-790be2cc1029</BLMJ>

        <CMD>Hello</CMD>

    </HEAD>

    <BODY>

        <SENDER OP="97252">+972506501020</SENDER>

        <CONTENT><![CDATA[Hello, world!]]></CONTENT>

        <DEST_LIST>

            <TO>6655</TO>

        </DEST_LIST>

    </BODY>

</PALO>
```

Example of a **HTTP/GET** MO message:

http://content_provider_url/xxx.asp?blmj=b21bc802-f28e-4962-9b1e-c0cec0948208&sender=%2B972523978686&recipient=6655&content=hello%20world&net=GSM&device_model=NOKIA6120&op=97252&date=201005131 51701

The BLMJ (Billing Major) tag is a unique identifier that is generated specifically for the message and allows further matching between the MO message and a possible response by MT message.

NOTE

Special characters which are not supported: &, <, >.

7. Reverse Billing Model

The Reverse Billing (RB) model enables the content provider to send a message to a subscriber and charge the subscriber for receiving the message. This is usually a premium charge of minimum 0.4 NIS per message.

The content provider should indicate the price of the mobile terminated (MT) message by using the BILLING section. The BILLING section should indicate the pricing plan in the RB tag. The RB tag actually sets the price to be charged from the subscriber. Cellact shall open a different pricing RB tag for every price that is required. The content provider must ensure that it has the correct pricing plan approved and working.

NOTE

When using a new pricing plan (RB tag) for the first time, send a test message and then verify with Cellact support mailto:support@cellact.com that the message was charged correctly.

7.1 Messaging Scenarios

NOTE

- **MO-MT transactions do not require an Electronic Signature (SIGI); they will be identified by the TRID tag (the BLMJ of the MO message).**

- **Renewable MT RB messages must include a valid SIGI in the TO tag.**

- **A one-time MT RB message must include a valid one-time SIGI in the TO tag.**

- **A MT RB message that will not include a valid SIGI will be blocked.**

- **Note that for some operators – any new service will need to be preapproved. The approval process may take several days.**

7.1.1 Renewable MT RB

Following is an example of a complete **sendtextmt** message with the **renewable SIGI** parameter:

```
<PALO>

    <HEAD>

        <FROM>Company_Name</FROM>

        <APP USER="UserName" PASSWORD="Password">LA</APP>

        <CMD>sendtextmt</CMD>

    </HEAD>

    <BODY>

        <SENDER>0506337000</SENDER>

        <CONTENT>Hello, world!</CONTENT>

        <DEST_LIST>

            <TO SIGI="a17d7878-b374-49f1-91ed-
453adcfaf731">0506501020</TO>

        </DEST_LIST>

    </BODY>

    <BILLING>

        <RB>CELLACT_01</RB>

    </BILLING>

    <OPTIONAL>

        <MSG_ID>1123528</MSG_ID>

        <SERVICE_NAME>News_alerts</SERVICE_NAME>

        <CATEGORY>SPORT</CATEGORY>

    </OPTIONAL>

</PALO>
```

Pay attention to the following fields:

■ **SIGI**: Inside the TO section, this tag indicates the valid Electronic Signature for renewable service.

■ **BILLING**: This tag indicates a Reverse Billing message.

■ **RB**: Inside the Billing section, this tag indicates the content provider's pricing plan.

■ **SERVICE_NAME**: An optional tag that can be used to identify the type of content for provisioning purposes. For example, if it is marketing content, a subscriber may wish to be blocked to this type of content.

7.1.2   Single MT RB

Following is an example of a complete **sendtextmt** message with the **one-time SIGI** parameter:

```
<PALO>

    <HEAD>

        <FROM>Company_Name</FROM>

        <APP USER="UserName" PASSWORD="Password">LA</APP>

        <CMD>sendtextmt</CMD>

    </HEAD>

    <BODY>

        <SENDER>0506337000</SENDER>

        <CONTENT>Hello, world!</CONTENT>

        <DEST_LIST>

            <TO SIGI="2450C55D-1A09-103B-9C8B-
0A7452B3F168">0506501020</TO>

        </DEST_LIST>

    </BODY>

    <BILLING>

        <RB>CELLACT_01</RB>

    </BILLING>

    <OPTIONAL>

        <MSG_ID>1123528</MSG_ID>

        <SERVICE_NAME>sports news</SERVICE_NAME>

        <CATEGORY>SPORT</CATEGORY>

    </OPTIONAL>

</PALO>
```

Pay attention to the following fields:

■ **SIGI**: Inside the TO section, this tag indicates the valid Electronic Signature for one-time service.

■ **BILLING**: This tag indicates a Reverse Billing message.

■ **RB**: Inside the Billing section, this tag indicates the content provider's pricing plan.

■ **SERVICE_NAME:** An optional tag that can be used to identify the type of content for provisioning purposes. For example, if it is marketing content, a subscriber may wish to be blocked to this type of content.

8.   MO/MT Model

Content providers who work in the **MO/MT model** (in which a subscriber sends a mobile originated message (MO), for example a request for an icon, and in return receives a mobile terminated message (MT) with the content, should add another field especially to support prepaid subscribers on the Orange GSM network. This method is recommended, since we expect that in the future the MO/MT transactions will be enforced by the mobile operators' policy that will check that the MT message is a response to a MO message.

The additional field used in the MO/MT model is the **TRID**, the Transaction Identifier. The field should match the BLMJ tag that is provided in the MO message. This means that once the content providers answer, the value of the BLMJ is copied and put it in the TRID field.

The **NET** attribute is used in case of a response to a MO message that arrives from the Cellcom network. The NET attribute indicates if it is a TDMA or GSM subscriber. In case of TDMA MO messages, the **TYPE** attribute should not be specified in the return message.

The content provider should respond within 12 seconds to Cellact in order to allow proper message delivery; otherwise the transaction may expire. If the transaction expires, the subscriber shall receive an automatic message from the mobile operator indicating that: "Message was not delivered, and therefore was not charged".

Here is an example of an MO/MT transaction. First, the MO message:

```
<PALO>
   <HEAD>
   <BLMJ> ab259538-91b7-480d-8ae0-790be2cc1029</BLMJ>
     <CMD>Example</CMD>
     <COMPANY>Company_name</COMPANY>
   </HEAD>
   <BODY>
   <SENDER OP="97254" NET="GSM">+972501234567</SENDER>
   <CONTENT>send me content</CONTENT>
     <DEST_LIST>
     <TO>6655</TO>
     </DEST_LIST>
     </BODY>
     <OTHER>
        <EVT>mo</EVT>
        <DATE>20080914114430</DATE>
        <CP_MO>ouch</CP_MO>
     </OTHER>
   </PALO>
```

The response from the content provider should be as follows:

```
<PALO>
    <HEAD>
        <FROM>Company_name</FROM>
        <APP USER="username" PASSWORD="123456">LA</APP>
        <CMD>sendtextmt</CMD>
        <TRID>ab259538-91b7-480d-8ae0-790be2cc1029</TRID>
    </HEAD>
    <BODY>
        <SENDER>6655</SENDER>
        <CONTENT><![CDATA[Here is your content]]></CONTENT>
        <DEST_LIST>
        <TO>+972501234567</TO>
        </DEST_LIST>
    </BODY>
    <BILLING>
        <RB>EXAMPLE1</RB>
    </BILLING>
    <OPTIONAL>
        <MSG_ID>1123527</MSG_ID>
        <SERVICE_NAME>news alerts</SERVICE_NAME>
    </OPTIONAL>
</PALO>
```

NOTE

- **In case of TDMA MO messages, the TYPE attribute should not be specified in the return message**
- **In case of MO MT flow, there is no SIGI identifier.**

9.   MOMMS Model

This mobile originated messaging model allows the content provider (CP) to receive rich content such as pictures, movies and recordings in image, video, or audio files. The CP decides the mode that it wants to receive the MO MMS message.

There are two ways to receive an MOMMS message:

- **Email**: An email is sent to an address that is decided by the CP. The email contains the BLMJ (Billing Major) value in the subject field, and the attachments of the email contain the content files that were sent by the mobile subscriber (end user).

- **MO message**: An MO text message is sent with the structure as shown in the example. Cellact stores the rich content on server for up to 3 days and sends a message that contains links to those files, enabling the CP to download the files. Under the Links tag, there is a link to each file that was attached to the message. That link can be used to download the files to the CP's own server.

Here is an example of a text message that is sent using the MOMMS model:

```
<PALO>
    <HEAD>
    <BLMJ>e2a383c5-0879-4031-8601-1c9ba9a8ab4b</BLMJ>
    <CMD>sendmms</CMD>
    </HEAD>
    <BODY>
        <LINKS>
        <LINK>http://mms.cellactpro.net/MoMMSFiles/b0316fe7-
8a72-azaz-a2a4-5ff811ecfe9e_.txt</LINK>
        <LINK>http://mms.cellactpro.net/MoMMSFiles/2ee1757a-
8300-az00-ba0c-c758afca9834_.jpeg</LINK>
        </LINKS>
        <SENDER OP="97252">+972541111111</SENDER>
    <DEST_LIST>
        <TO>7541</TO>
    </DEST_LIST>
        <CONTENT>mo from vmail</CONTENT>
    </BODY>
    <OTHER>
        <EVT>mo</EVT>
        <DATE>20080819142520</DATE>
        <CP_MO>cellcom</CP_MO>
    </OTHER>
</PALO>
```

10. Appendices

10.1 Code Example

Here is an example of a VB script for an MT SMS message:

```vb
Dim args
Set args = WScript.Arguments
Set winObj = CreateObject("WinHttp.WinHttpRequest.5.1")
' Also you can use HTTPS
Call winObj.Open("POST",
"http://la.cellactpro.com/unistart5.asp", False)
winObj.Option(WinHttpRequestOption SslErrorIgnoreFlags) = &H3300
'Set request header.
winObj.setRequestHeader "User-Agent", "Message Test"
winObj.setRequestHeader "Content-Type", "application/x-www-form-
urlencoded"
'Build the XML for sending
lsXml="<PALO><HEAD><FROM>Company_Name</FROM><APP
USER=""User_Name""
PASSWORD=""Password"">la</APP><CMD>sendtextmt</CMD></HEAD>"
lsXml=lsXml & "<BODY><SENDER>int_number</SENDER><CONTENT>" & "
Test message" & "</CONTENT><DEST_LIST>"
lsXml=lsXml & "<TO>0501234567</TO>"
lsXml=lsXml & "</DEST_LIST></BODY>"
lsXml=lsXml & "</PALO>"
'Call Replace Data
lsXml = ReplaceData(lsXml)
'Concatenating the XMLString to its paramater
SendString = "XMLString=" & lsXml
winObj.send (SendString)
'Print Response
result=winObj.responseText
wscript.echo result
'Replace Problematic Chars
Function ReplaceData(ByRef data)
data = Replace(data, "%", "%25")
data = Replace(data, " ", "%20")
data = Replace(data, "#", "%23")
data = Replace(data, "&", "%26")
data = Replace(data, "?", "%3F")
data = Replace(data, "+", "%2B")
ReplaceData = data
End Function
```

10.2   Acronyms

Table 6 lists the acronyms that may be used in this document.

Table 6: Acronyms

Acronym	Definition
BLMJ	Billing Major
CP	Content Provider
EVT	Event
GSM	Global System for Mobile Communication
GW	Gateway
LA	Large Account
MO	Mobile Originated (transaction)
MMSC	Multimedia Message Service Component (network)
MNP	Mobile Number Portability
MT	Mobile Terminated (transaction), Message Type
RB	Reverse Billing
SM	Short Message
SMS	Short Message Service
SMSC	Short Message Service Component (network)
SMPP	Short Message Protocol
SMTP	Short Message Transfer Protocol
TDMA	Time Division Multiple Access
TR	Transaction (as in TR_ID)
TTL	Time To Live
TTS	Time To Schedule

Contacting Cellact

Cellact is committed to customer service and support.

Contact us at: mailto:support@cellact.com

Phone: +972-9-9704181

Cellact Ltd.

Shefayim Business Center

P.O. Box 286

Shefayim 60990 Israel

Tel: +972-9-970-4110

Fax: +972-9-970-4210

Visit our website:

http://www.cellact.com or http://www.cellact.co.il