Tender Documentation: 2-way SMS Overview

2-way SMS Overview

email message to a SMS receiver þ the SMS reply message to the original sender as email

1 Introduction - Overview

1.1 DESCRIPTION

"2-way SMS messaging", or '2-way email to SMS messaging', enables a <company> customer to email a message to an SMS device, typically a cellphone, and for that cellphone user to *send a reply back to the <company> customer's email address*. Earlier (one-way) SMS messaging never enabled a receiver of an email-to-SMS message to send a reply SMS back to the originating email address.

1.1.1 HOW 2-WAY SMS WORKS

Initially each 2-way SMS customer must be appropriately set up in both <system 1> (<company>'s customer management and billing system) and in <system 2>. After this has been completed they can then utilise <company>'s 2-way SMS messaging services.

Sending an email to an SMS cellphone:

1. Using their email application, the <system 2> customer sends an email to the address:
   <destination cellphone number>@sms.aaa.bbb.com
   e.g.: 0444777333@sms.aaa.bbb.com
   There are a couple of variations on this addressing scheme that we will discuss later.

2. Once received by the <system 2> system, the email is assigned a "temporary" cellphone number from a pool of 200 (real) cellphone numbers set aside for this task.

3. The email subject and message, the 'from' email address, the allocated temporary cellphone number, and the destination cellphone number are recorded in a database table (mds2wse).

4. The 'cellphone' SMS message is transmitted to an SMS carrier (e.g. Optus, Vodaphone) from where it is delivered to the destination SMS cellphone.

Replying from an SMS cellphone back to the correct email address:

5. Using the 'reply' functionality of their cellphone, the recipient construct a (reply) SMS message *from* themselves, *to* our original emailing <company> customer. This is a message to be sent to the allocated temporary cellphone number

6. This new reply message is received by the SMS carrier (e.g. Optus, Vodaphone) and transferred on to <company>.

7. The <system 2> system extracts the 'from' and 'to' cellphone numbers from the message header, using them to find the appropriate return email address from the database where they were stored earlier.

8. <system 2> now can, and does, construct and send the reply email. The email's "To:" address is extracted from the database record we have just located, the reply SMS message supplies the email's text, and "Reply from Mobile# *mobile number*" is used as the email's subject.

9. The email is sent by the <system 2> system and is received in the customer's email account shortly afterwards.

1.2 BENEFITS

- *Simple, easy and quick way to set up a mobile phone messaging service*
- *No special software, hardware, training or support required*
- *Turns any e-mail system into a mobile phone messaging service.*
- Sources of Email messages may change transparently, that is, without affecting or even the knowledge of, the message recipient. Over time one's, or the appropriate staff's, or a company's source email addresses will all change.
- A <company> customer can easily adjust its own systems to automatically send 2-way SMS messages. Most customers, with only simple software development, can already make any modern computer system send an email. Now, using the <company>'s 2-way SMS system, this email can be delivered as a 2-way SMS message, both
  - arriving instantly on the recipient's cellphone
  - accommodating the message recipient's reply
- Instantaneous, buffered, recorded, text-based 2-way messaging is now available between any organisation / company / corporation and any SMS phone owning individual; employee, customer, and / or independent individual

1.3 CONCEPTS

Carrier A company that owns a Telecommunications transmission network. <Company> operates as a pager message carrier for other telecommunications companies, while using <external telco 1> and <external telco 2> as carriers for its SMS messages.

Provisioning The allocation of a new phone-number, and the process of making other telecommunications companies aware of the new telephone number

SMS The text-messages we all send and receive on our cellphones.

SMSC The part of the telecommunications carrier that deals with SMS messages.

2-way SMS: Customer Side

2 Customer's I.T. requirements (hardware / software)

The customer needs
- a computer connected to the internet, and
- an application to manage the sending and receipt of email.

These days most people, and especially companies, have access to such resources.

3 How the customer is to use 2-way SMS

3.1 Addressing 2-way SMS emails

The addressing rules for 2-way SMS email are the same as for 1-way, standard, email-to-SMS messaging.

3.1.1 Standard <company> 2-way SMS email addressing

The standard, default way to address emails for the <company> 2-way SMS system is as follows:

<*destination cellphone number*>@sms.aaa.bbb.com

Thus, if I wished to send a 2-way SMS message to the cellphone 0444-777-333, I would, after registering with <company>, address my email to:

0444777333@sms.aaa.bbb.com

3.1.2 Addressing by PIN-secured 2-way SMS customers

A security option available to <company>'s 2-way SMS customers is for their emails to be PIN protected. PIN protection shields the <company> customer's account from incurring the cost of emails sent by other, malicious, actors who may have altered the 'from' address of their emails so that they become the same as the email address of someone that they (the malicious actor) knows to be a true 2-way SMS customer. Altering the 'from' address of an email is trivial.

PIN protection involves embedding a secret, 4-digit PIN number into the 'To:' address of the email, giving the email address the form:

<*destination cellphone number*>-<PIN>@sms.aaa.bbb.com

Thus, if I wished to send a 2-way SMS message to the cellphone 0444-777-333 and my pin was 1111 I would address my email to:

0444777333-1111@sms.aaa.bbb.com

3.2 EMAIL TESTING AND SECURITY AUTHENTICATION

The series of tests undertaken on each email arriving for conversion to a 2-way SMS message are detailed in this section. These tests are of two types:

- Format and integrity of the email message. Are we able to convert the email to a 2-way SMS?
- Security and Authentication. Will we allow this email to be converted and sent?

3.2.1 THE EMAIL CHECKING PROCESS (SUMMARIZED)

First the system tests and approves the email's format and integrity

1. Test and approve the format of the phone number in the 'To:' field of the 2-way SMS message
2. Test and approve the phone number destination.
3. Test and approve the data held in the email. Is it only text?
4. Open the email and process the email's text.

If, and only if, the format of the email is correct, separate cumulative levels of authentication are the next hurdles, of which one must - and up to three may - be passed.

5. Authenticate the sender, or the entire domain
6. Authenticate the email gateway from which the email was sent.
7. Authenticate a 4-digit PIN number embedded into the email "To:" address

All emails must pass the first test, the authentication of the sender / domain. Individual customers can then elect to have either the second or the second and the third levels applied.

3.2.2 EMAIL FORMAT AND INTEGRITY

3.2.2.1 Overview

Before bothering with any processing or security checking, <system 2> tests that the email itself makes sense as a potential 2-way SMS message. A number of tests are run, tests that, over time, will change as SMS messaging capabilities are extended.

3.2.2.2 Rules and implementation

The tests are carried out in the following order, the email being rejected on the first test failed.

1. Does the phone number embedded in the email's "to:" field appear to be in a permitted format?
2. Is it a phone number to which we can, and wish to, send an SMS message?
   (e.g. Alaska is not currently serviced by <company>)

   Using our earlier example, 0444777333@sms.aaa.bbb.com, we test:
   - that it neither too long, nor too short
   - that, with a zero, the second number is '4'
   - that any international dialling code prefixing the number is acceptable

3. Is the email constructed of data we can process?

   Only simple text-emails are processed at the time of writing, though the types of emails handled will most likely expand over the next few years. This test ensures that the email exists and that it has at least one MIME component: the body of the message. An empty, blank message will still contain one component.

4. Compile, clean and process the email text

   No errors should be generated here, though the characters "empty message" will replace any empty message. More details appear in the next section ("SMS Message Generation")

3.2.2.3 Informing the user of Formatting and Integrity Failures

Error	Message
Phone number format incorrect	"Reject: Invalid format number"
MIME type unsupported: incorrect email data	"Reject: unsupported content type= MIME-Type"
Message corrupt: no MIME components	"ERROR: MIME contains no data"

The user is not notified that their message is found to be of zero length after the unprintable characters and consecutive spaces are removed.

3.2.3 SENDER / DOMAIN AUTHENTICATION

3.2.3.1 Overview

Either the complete email's 'from:' address or just the domain of every email destined for 2-way SMS messaging must be authenticated:

> the full email address of the sender (the "from:" field) is looked for in the <company> A-Party database table. If a match is found (ignoring upper and lower case) the <system 2> 2-way SMS system authenticates the email's sender.

Many customers will have their security needs fully met by this authentication test. Others, however my require more security, and will chose one or both of the additional two security checks.

NB: It is, effectively, trivial to alter the "from:" address of an email that one sends, and thus a malicious actor could send a 1 or 2-way SMS message[1], charging this transaction to the <company> customer. Any customer desiring a strong assurance of security should consider adopting one or both of <company>'s additional security checks.

3.2.3.2 Rules and Implementation

Specific Customer Search

Taking a copy of the 'From:' address from the email, the A-Party database table is searched for a record containing both:

- the customer's email name: the 'joe' of 'joe@mycompany.com.au', and
- the customer's email domain: the 'mycompany.com.au'.

If this record is found:
- and the status field indicates that the customer is active: Success.
- and the status field indicates that the customer is suspended: Failure.

[1] A two-way message would be problematic however. Having spoofed the "from" address to send the email for free, this email address becomes the destination address of any reply, the true <company> customer possibly receiving replies to messages that they have never sent. An associated issue is that any 2-way SMS customer receiving replies to messages that they did not send should notify <company> immediately.

If the record is not found:

we try to find a record indicating that the whole domain has permission to send 2-way SMS messages before rejecting the customers message. See the following.

Domain Search

If the previous search for the complete email address failed, the A-Party table is searched again for a record containing only the domain name (e.g. 'mycompany.ccc.com) plus an empty email name, indicating that anyone from the specified domain can send 2-way SMS.

If such a record is found,

- and the status field indicates that the whole domain is active: Success.
- and the status field indicates that the whole domain is suspended: Failure.

If the record is not found: Failure.

- the customer may not use the <company> 2-way SMS service. They have neither a specific permission (via their email address appearing in the A-Party table) nor does their email domain have blanket permission.

3.2.3.3 Informing the user of Authentication Failure

Upon authentication failure, an email reply is automatically sent to the email initiator, informing them of their error.

Error	Message
Full email address found in the A-Party table Status Field indicates the account is not active	"Your account is currently inactive."
Email domain (only) found in the A-Party table Status Field indicates the account is not active	"Your account is currently inactive."
Neither full email, nor domain, in the A-Party table	"Your account has not been registered for this service."

3.2.4 EMAIL GATEWAY AUTHENTICATION

3.2.4.1 Overview

Email Gateways

When talking about email, a 'gateway' refers to one of more of the machines through which the email has passed en route to its destination. The 2-way SMS 'email gateway authentication' looks for a specified gateway – usually the customer's own email server – in the 'header' of the received email.

Email Headers

Each email one receives includes a (usually unseen) 'header', within which some version of the entire journey that the email has traversed is recorded. To authenticate that the email message came from the correct place, the email gateway used by the customer is searched for in the data in this header.

To see an email header in a Microsoft Outlook email,

1. Open an email you have received
2. make sure that the View > Message Header is selected
3. Click the 'Options' tab above the email message but beneath the menus.

The lower half of the page displays the email's header. It is in here that the specified email gateway must be found.

This 'email gateway authentication' test is much harder to violate than the compulsory 'from:' field address check.

3.2.4.2 Rules and Implementation

When an email is received, its 'from:' address indicates which <company> customer the email is from, and thus which A-Party record (in the mdsaparty database table) holds the sending customer's information. One of the fields in this database record, "**gateway_domain**", is used to implement the 'email gateway authentication' test.

- First, if the "gateway_domain" field is empty, this test is not to be undertaken for this customer. If they have passed the earlier 'from:' field authentication test their email is now 'authenticated', and, without further a-do, will be sent as a 2-way SMS message.

- If this "gateway_domain" field contains an entry, this string must appear in the email's header. If it does, the email passes this test. If it doesn't, the email is rejected.

3.2.4.3 Informing the user of Authentication Failure

If this 'email gateway authentication' test is applied to an email and fails, the user receives a reply email containing the following message:

"Your account not allow to send through the email gateway domain." [*sic*]

Possibly, some of these error messages will be updated.

3.2.5 PIN NUMBER AUTHENTICATION

3.2.5.1 Overview

The third layer of authorisation is the testing of a 4-number PIN embedded in the email address. As detailed above, customers using this method will address their emails as

<*destination cellphone number*>**-**<PIN>@sms.aaa.bbb.com

Thus, if I wished to send a 2-way SMS message to the cellphone 0444-777-333, my pin was 1111 (a bad choice) I would address my email to:

0444777333-1111@sms.aaa.bbb.com

It is up to the customer to make derivation of the PIN as difficult as possible for third parties.

3.2.5.2 Rules and Implementation

Similar to the previous 'gateway' test, and using the same database record, the current PIN test compares the PIN embedded in the email address with the contents of the "**pin**" field in the extracted A-Party database record.

- If the "**pin**" field in the extracted A-Party database record is *empty*, this test is *not* to be applied. If the previous tests have been passed, the email is now 'authenticated' and is converted to a <company> 2-way SMS message

- If the PIN both exists and matches the "pin" field; success. Again the email is now 'authenticated' and is converted to a <company> 2-way SMS message.

- If the PIN does not match the "pin" database field; failure: the email is rejected, and a failure email is returned to the sender

3.2.5.3 Informing the user of Authentication Failure

If the PIN test is applied and fails, the customer is informed of the authentication failure by an email, the customer's 2-way SMS email being deleted.

The customer receives the message:

"Invalid PIN."

3.3 SMS MESSAGE GENERATION

3.3.1 MESSAGE TEXT

The message to the SMS phone is constructed from the emails
(1) Subject line, plus
(2) email message text, and
(3) the name of any attached file.

In more detail the SMS message generation rules are as follows:
- first the subject line (if any) is prefixed to the email message text. Thus the subject line of the email is no different from the email message's text
- next the name of any attached file is appended to the end of the text string generated so far as <<filename.extention>>.
- Any control characters (e.g. end-of-line), multiple spaces and other junk are converted to single spaces, ensuring that only printable characters are delivered.
- If the message is now empty, or consists of only spaces, it is re-set to the characters: "blank message"

3.3.2 MESSAGE LENGTH

As a maximum the length of the message string to be transmitted will be fixed at 160 characters, truncation occurring if the constructed message is longer than 160 characters. This is a limitation imposed by the SMS format and the carriers.

3.4 MESSAGE QUANTITY AND LIMITATIONS

3.4.1 EXCESSIVE MESSAGING

From each domain, only 300 emails every 2 minutes will be processed, after which the customer (domain) is blocked for a period of time, say 20 minutes. This blocking occurs outside of the 2-way SMS system, at the email server level, part of <system 2>.

3.4.2 TIME LIMIT ON REPLIES

2-way SMS messages are stored in <system 2> for 'N' days, 'N' probably set in the range of 7 to 10 days. As a result, it is not possible for replies made outside this timeframe to be transmitted back to the <company> (A-Party) customer's email address, as the record of the originating email address will have been deleted.

This 7 to 10 day limit (say) is dependent on Hard Disk size – the amount of space we are happy to allocate to store this data.

3.4.3 LARGE, BUT LIMITED, 'CORRECT' REPLIES

When an email is converted into a cellphone message and sent as an SMS, it is allocated one of the 200 cellphone numbers owned by <company> specifically for this purpose. Further, a record of this message, indexed by this allocated cellphone number and the destination number, is made in the mds2wse database table, along with the message text and the originating email address. Obviously, every time someone sends a 2-way SMS message they are allocated one of these 200 cellphone numbers as the 'pretend' cellphone from which the email originated.

Less obviously, each time a message is sent from a particular single email address to the same particular, single SMS cellphone, the email address is allocated to a different 'pretend' cellphone number. This is so that each message from this particular emailer to this particular SMS cellphone owner can be individually identified.

The result of this is are as follows:

1. a particular, single email address can send up to 200 messages to the same particular, single SMS cellphone, before the number of 'pretend' cellphone numbers has been exhausted (as a different cellphone number was allocated each time).
2. Once the supply has been exhausted the first cellphone number is used again as the 'pretend' originating cellphone number
3. Replies to the 200-messages ago old first email-to-SMS message will now appear to be made to an incorrect message

Note: As the old messages are cleaned out (each week), the originating 'pretend' cellphone numbers become again available, and thus the likelihood of the problem as per point 3 above disappears.

Thus one must send:

- 200 Email-to-SMS messages
- to the same single SMS cellphone number
- within a 7 to 10-day period

for there will be any problems.

So, in conclusion, while this scenario is unlikely it could, one day, occur.

4 Transmission of the 2-way SMS message

4.1 SENDING THE SMS MESSAGE

Emails are received by <company>, passed through the <system> I system as internally formatted messages and delivered to a the skymds11t program that sends them on to a telecommunications carrier SMSC (SMS Centre).

As a simple overview, the process is similar to the following:

1. The customer's email is received by the <company> email gateway program mdsemgw. mdsemgw spawns a copy of sendmail to retrieve each incoming email.
2. The email 'from:' address is tested against the email domain blocking table. This table contains records indicating the email addresses and domains to be blocked from sending email to the <system 1> and <system 2> systems.
3. mdsemgw transfers the email to a holding queue.
4. The A-Party email processing program, mdsem02, extracts the email from this holding queue and applies all the tests specified in the "Email Testing and Security Authentication" section above.
5. Passing these tests, the email is transferred to the "Bulk SMS" queue, which actually handles both bulk and normal / single SMS messaging.
6. One of the two copies of skymds20 is dedicated to servicing this "Bulk SMS" queue. skymds20 extracts the message containing the SMS text from the "Bulk SMS" queue, and inserts it into the appropriate 'distribution' queue. Currently there are only two relevant queues:
   - SAU: the SMS / Australian queue
   - SNZ: the SMS / New Zealand queue
7. skymds03, the second largest <system> program, manages the transference of messages from distribution queues to destination delivery systems, e.g. from the fax message queue to the fax server. In our case, copies of skymds03 (especially configured) extract messages from the SAU and SNZ queues, delivering them to the skymds11t program. It is this program, skymds11t, which delivers the email/SMS message to the telecommunications carrier[2].

4.2 TRANSMISSION OF THE SMS TO THE TELECOMMUNICATIONS CARRIER

skymds11**t** transfers the SMS messages to the telecommunications carrier's SMSC (SMS Centre), which transmits the SMS on to the appropriate destination cellphone. Upon receipt of the SMS by said cellphone, both a reply receipt message and optionally a reply SMS from the cellphone's owner are transmitted back, via the carrier's SMSC, to the <system 1> skymds11**r** program.

When skymds11t receives the <system> message, it first assigns the to the email one of 200 cellphone numbers as its 'pretend' originating telephone number. After doing this, it writes a record to the mds2wse database table, recording:
- this 'pretend' originating cellphone number
- the (real) destination cellphone number
- the originating email address
- the message sent
- other technical data

skymds11t now sends the message to the SMSC, the telecommunications carrier's SMS Centre.

The rest is as described before. From the SMSC, the SMS message travels to the recipient's cellphone. There he or she reads the message and, let's say, chooses to send a reply SMS message[3]. The message comes back to the telecommunications carrier's SMS centre, which sends it to <company> where the skymds11r program receives it.

[2] This is different from most other <system 1> systems, where xyz directly transmits the message to the delivery mechanism.
[3] If they choose to call the sender, they receive a "Currently switched off or unavailable" message.

4.3 DELIVERY OF REPLY MESSAGE(S) TO THE ORIGINAL EMAIL SENDER

As just noted, skymds11r, essentially a simple opposite of skymds11t, receives the reply messages - both "delivery receipt" messages (to emails) and the SMS recipient's optional reply message. skymds11r stores each reply in the mds2wr database table.

The next step is for mdsemr to construct the reply email:

1. using the 'from' and 'to' cellphone numbers, mdsemr looks up its appropriate record in the mds2wse table
2. once the record is obtained mdsemr extracts the email address and original email message
3. If the message is simply a delivery receipt, the email address and original email message are used to construct the delivery receipt. If this is a proper SMS reply, the SMS text is included and the email formatted to appear as a genuine email reply – which, in fact, it is.
4. before sending, mdsemr writes a CDR for the email, so that the A-Party customer is billed appropriately.

Finally mdsemr writes to the "Bulk SMS" queue, for the email to be transferred on to its originator.

5 Types of replies a user may receive

There are three types of email reply you can receive in response to a <company> 2-way SMS message:

1. A delivery receipt email from <company> and the SMSC.
   You will <u>always</u> receive one of these.

2. A genuine reply from the SMS recipient.
   You will <u>often</u> receive one of these, but if (and only if) the SMS recipient chooses to reply.

3. An error message from the <company> system.
   You will <u>occasionally</u> receive one of these is email you send is incorrectly formatted or does not pass the <company>'s security and authorisation requirements.

5.1 DELIVERY RECEIPTS

Delivery receipts:
- are used to indicate that an email's SMS has made it to a cellphone,
- won't arrive until the SMS destination actually receives the SMS message
- are received in the skymds11r program as SMS messages
- end up as email messages courtesy of the mdsemr application

After completion, the delivery receipt is transferred via the Bulk SMS queue to the originating email address. There are two 'Status'es possible for delivery receipts:

Status	Meaning	Description
'DELIVERED'	success	The message has been delivered.
'UNDELIVERABLE'	failure	The message could not be delivered in the maximum possible time

5.1.1 EXAMPLE 2-WAY SMS MESSAGE DELIVER RECEIPT

As an example, your delivery receipts will look something very much like the following:

Subject:
Delivery Receipt from Mobile# 61422561191

Message:
Delivery Receipt:

Status: DELIVERED
Destination: 61422561191
Submitted: 11/03/03 14:34
Received: 11/03/03 14:34
Message:
Hi Nick. I'm @ Sara's. See you there soon. Please bring the sample.

5.2 REPLY FROM THE SMS DESTINATION

The receipt of email replies from SMS mobile phones is the *raison d'être* of 2-way SMS messaging. This technology has been made possible, within <company> at least, by

- the conversion, with-in <system>, of the email message to an SMS
- the allocation of one of 200 cellphone numbers to each 2-way SMS email,
- the reply SMS being transmitted to this cellphone number.

Format of returned message

5.2.1.1 Example 2-way SMS message reply

Subject:
Reply from Mobile# 61422561191

Message:
On way, there by 4. Bringing samples. N

---Original Message--- Sent: 11/03/2003 14:34
Hi Nick. I'm @ Sara's. See you there soon. Please bring the sample.

5.3 ERROR NOTIFICATION FROM <SYSTEM>

5.3.1 BLOCKING MESSAGES

- You have been temporarily blocked from this service due to excessive use. Any subsequent emails will be ignored.
- You have been permanently blocked from this service. Any subsequent emails will be ignored.

5.3.2 ACCOUNT PROBLEMS

- Subscriber Id does not exist or is currently inactive.
- Subscriber Id is invalid format
- Email messaging not enabled for requested subscriber.
- Your account has not been registered for this service.
- Your account is currently inactive.

5.3.3 AUTHORISATION / SECURITY FAILURE

- Bulk SMS Email attachment does not conform to the agreed specification.
- Bulk SMS Email contains more than one attachment and cannot be processed.
- Bulk SMS attachment content error - Line#
- Invalid PIN.
- Invalid Batch Number.
- Your account not allow to send through the email gateway domain. [*sic*]
- Your account has no permission for this Escalation/Roster.
- Email message not processed due to message containing no data

5.3.4 SAMPLE ERROR MESSAGE

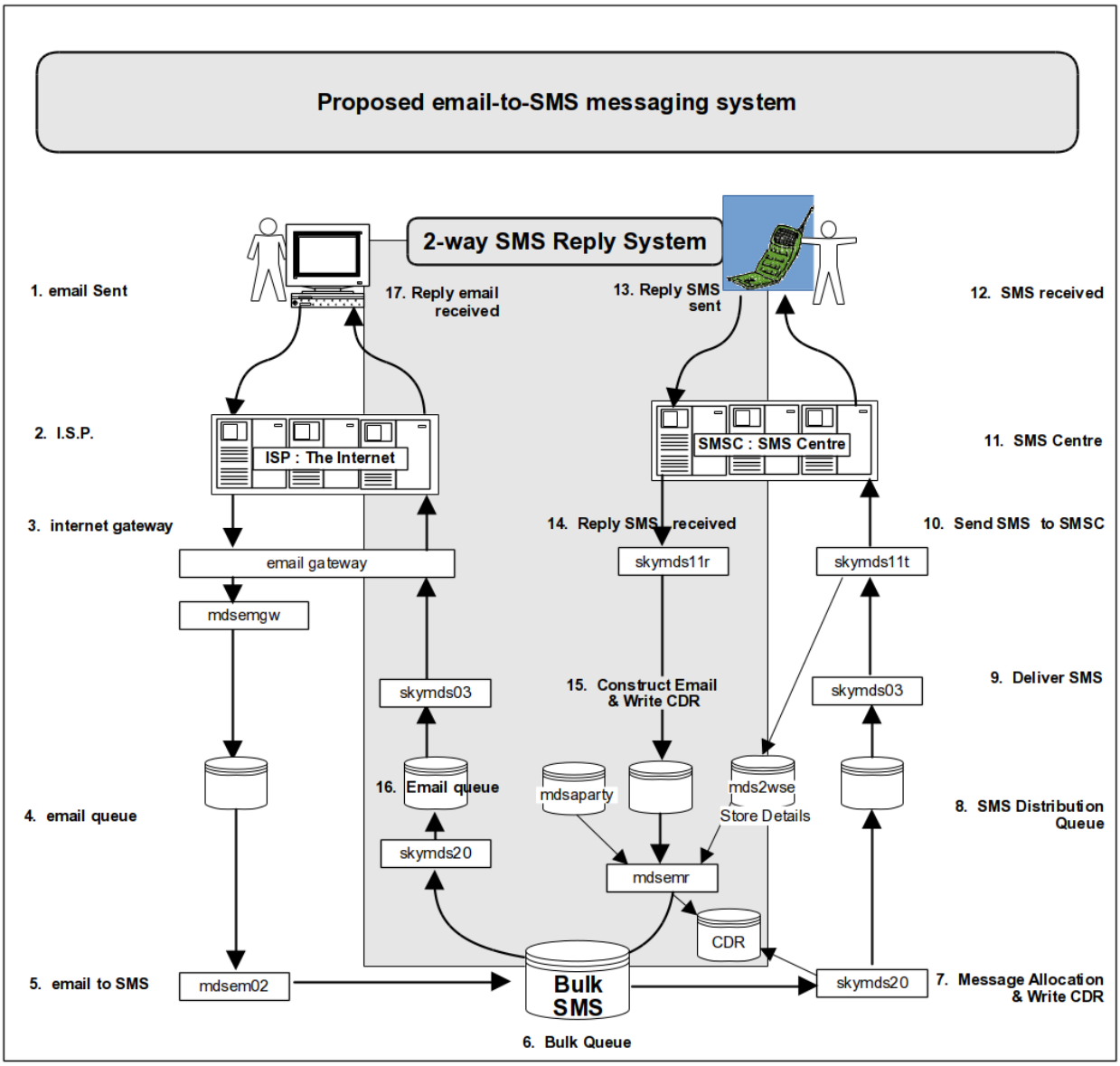
Note that the error message appears as a "Status:" line in the error email.

Subject:
Message Failed

Message:
Subscriber ID: 0422914276 [← This is actually the destination phone number]
Date: 13/03/2003 17:47:08 EDT

Status: Your account is currently inactive.

5.3.5 SIMPLE DIAGRAM OF THE 2-WAY SMS PROCESS



2-way SMS: <company> Side

6 <company>'s maintenance of a 2-way SMS customer

6.1 MONITORING 2-WAY SMS MESSAGE TRAFFIC

All of <company>'s email, and thus the entirety of its 2-way SMS message traffic, passes through the <system> (lnklo) machine and, on this machine, writes log messages to the current day's email log file. Each of these daily log files is named after the Year (YY) month (MM) and day (DD) plus the string 'emgw' (email gateway), to generate a file name such as emgwYYMMDD, e.g. emgw090226.log for the 26th of February 2009.

These logfiles reside in lnko's /var/mds/data/email/logs/ directory, those for the previous fortnight being kept.

6.1.1 2-WAY SMS MESSAGE EMAIL LOG SAMPLES

The following are the three log entries (in /var/mds/data/email/logs/emgw030312.log) made by a 2-way SMS message sent on the 12th of March 2003.

MDSEMGW Ver: 2.00.5 12/03/2003 13:17:13 Recd: 0422914294@sms.aaa.bbb.com, From: smcgregor@<company>.com.au
MDSEMGW Ver: 2.00.5 12/03/2003 13:17:13 0422914294@sms.aaa.bbb.com, from smcgregor@<company>.com.au status [Queued to <system>]
MDSEM02 Ver: 2.01.7 12/03/2003 13:17:13 0422914294@sms.aaa.bbb.com, from smcgregor@<company>.com.au status [Despatch to <system>]

- The first records the email message being received by <company>'s email gateway (mdsemgw – "Recd").
- The next records the email being queued for dispatch from the email gateway ("Queued to <system>")
- The last records the email arriving at the program that is to process it, in this case mdsem02, the A-Party Email and SMS processor.

6.2 BLOCKING (UNBLOCKING) 2-WAY SMS MESSAGE CUSTOMERS

6.2.1 OVERVIEW

For various reasons - excessive-use, brief suspension for the customer's own testing, spam, illegal use - <company> (i.e. <system>) suspends access by customers to its email system. These suspensions are enforced for differing lengths of time depending on the customer's attributes and behaviour. Usually, but not always, the user is notified (by return email) that their message has been blocked from traversing <company>'s email system.

Note that a customer can be blocked (and unblocked) both by the <system> system (i.e. automatically), and by <company>'s staff (manually).

6.2.2 EMAIL BLOCKING IMPLEMENTATION

The <system> email blocking records are held in the 'mdsemblk' database table. A user interface to this database table, and thus to the email blocking system as a whole, is supplied by the identically named <system> 'mdsemblk' program.

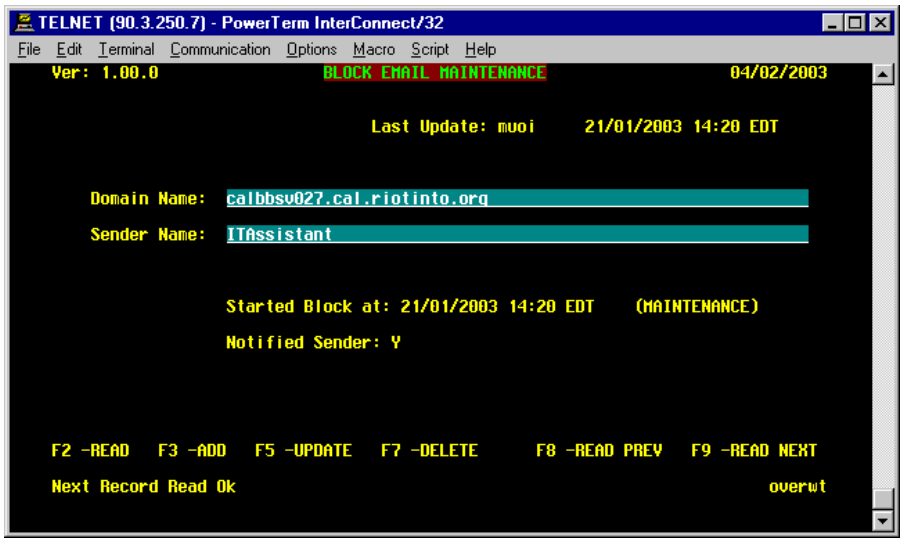
6.2.2.1 'mdsemblk' database table

The mdsemblk database table contains all the <company> email blocking data. The data it holds is as per the following table:

Field Name	Description
domain_name	Sender's email domain name (e.g. 'myCompany.com.au')
sender_name	Sender'email name (the 'Jo_Smith' of 'Jo_Smith@myCompany.com.au')
initiator	Is this manually or automatically generated?
notified_sender	Has the email sender been notified that their emails are blocked?
block_date_time	When was the block initiated?
operator	If manual, who initiated the block?
mod_date_time	When was this record last modified

6.2.2.2 'mdsemblk' email blocking maintenance program.

A user interface to the <system> email blocking system is supplied by the 'mdsemblk' program, accessible via <system> > 'File' menu > "Email Blocking Maint" menu item. This program can both set and delete email-blocking records.



As can be seen, this program displays the fields of the mdsemblk database table, the domain name (e.g. myCompany.com.au) and the sender name (e.g. the 'Jo_Smith' of 'Jo_Smith@myCompany.com.au') are available for editing. One can add a new record, accept the defaults, or enter the domain and an optional email sender (F3), or can update an existing record (F5). Note again that the 'Sender Name' field is optional and, if not entered, the entire domain is blocked.

Each time a manual addition of a blocking record is done, the 'Notified Sender' field is set to 'N', indicating that the user is blocked but that they have not yet been notified of the block. The first time they subsequently have any email rejected from the <system> system because of this blocking record they are emailed one single time, and the 'Notified Sender' field is automatically changed to 'Y'.

6.2.3 UNBLOCKING BLOCKED EMAIL DOMAINS

6.2.3.1 Unblocking automatically blocked email domains

After an hour, each automatically blocked domain is released. The mdsemblk database table is processed and for each automatically generated blocking record, the block_date_time field is tested. If this timestamp is greater than one hour in the past, the record is deleted.

The '1 hour' life expectancy for blocking records can be adjusted easily. It is set as a command-line parameter.

6.2.3.2 Unblocking Manually blocked email domains

The only way to unblock any manually blocked email addresses or domains is via the mdsemblk program.