INTERNET-DRAFT Jeroen Houttuin
RARE WG-MSG RARE Secretariat
rev. 2.1 March 1993

Recommendations for Mail Based Servers

Abstract

This document defines recommendations to be implemented in mail based servers in the Internet e-mail community. The requirements only affect the basic behaviour of servers, i.e. it mainly deals with how header fields are handled. Although there is also a clear need for recommendations in the field of end user requirements, such as command syntaxes for archive servers, automatic distribution list subscription, etc., such issues are considered more suitable to be dealt with in a separate document.

It is highly desirable that other e-mail networks connected to the Internet, such as the GO-MHS community, also implement these recommendations.

Discussion group

This document is being discussed in the RARE Working Group on Mail and Messaging (WG-MSG) and in the IFIP Mail Management Group. Please send any comments to wg-msg@rare.nl or to houttuin@rare.nl .

Status of this Memo

To do: more comprehensive explanations for the individual recommendations. Finish the explicit parallel descriptions in both RFC and X.400 terminology.

This document is an Internet Draft. Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its Areas, and its Working Groups. Note that other groups may also distribute working documents as Internet Drafts.

Internet Drafts are draft documents valid for a maximum of six months. Internet Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet Drafts as reference material or to cite them other than as a "working draft" or "work in progress."

Please check the I-D abstract listing contained in each Internet Draft directory to learn the current status of this or any other Internet Draft.

Distribution of this memo is unlimited.

Contents

1. Introduction

Mail Based Servers

Electronic mail systems are increasingly being used as a basis for so called Mail Based Servers (MBSs), such as echo servers, distribution lists, etc. MBSs are used for a number of purposes:

- Enhancing the Message Handling Environment. Examples of such usage are distribution lists (DLs), for group communication, and e-mail servers, for file and information retrieval.

- Monitoring the status of the MHS. Examples of this usage are echo servers and forced (non-)delivery messages (E.g. the so-called nosuchuser test).

Since MBSs deal with automatically receiving, forwarding and replying to messages, which may themselves have been generated by automated processes, strong requirements are needed on the one hand to minimise human effort to manage such servers, and on the other hand to make the behaviour of mail based servers deterministic enough to build reliable tools upon them.

A classic example of what can go wrong is when a mailing list contains an invalid address. The remote mailer generates a non-delivery message and sends it to the originator of the original message, which, under circumstances, could be the list itself, which then again distributes the non-delivery message to the non-existing recipient, etc. Following strict recommendations on how mailing lists should handle message header fields can avoid such looping-endangered situations.

A more complicated example of the usefulness of strong requirements for mail based servers is the following: suppose a distributed tool will check the connectivity of mailers by sending a message to an echo-server. The connectivity tool could request the echo to be sent to a remote component of the tool instead of to itself. If for some reason the address of that other component cannot be routed to, an automatically generated non-delivery message could be sent back to the echo server, which results in an echo loop.

The recommendations defined in this document will as much as possible be aligned with comparable rules that either have already been used for a long time (X.400(84) Status Reports; distribution lists in the Internet), or are already defined in other documents (X.400(88) DLs).

Approach

If all MBSs would agree to implement a common set of recommendations, this set could be fairly small. In practice however, there are some reasons why such a 'minimum approach' will not work:

- The most obvious reason is that one cannot realistically expect all networks and software developers to implement one common strict set of rules. In different mail communities, different MBS conventions have already been used for a long time. Some of these conventions can be unacceptable for other communities to implement.

- MBSs can be build upon different underlying protocols. For instance, it is almost impossible to have one small set of rules that will prevent problems between any combination of MBSs, e.g. between an RFC 822 MBS running over NJE and a P1 based MBS. More problems can be expected because header fields are crucial for the properly functioning of MBSs, and protocol gateways will not always map header fields bijectively.

- Not all MBSs are controlled by software developers or network operators. Any user can write a simple program that will have the functionality of an MBS.

Because the 'minimum approach' is not feasible, this document recommends the 'unilateral safety approach'. The idea is that any MBS that implements the complete set of recommendations will be safe from harm, regardless of what other 'dumb' MBSs it is interacting with.

This results in quite a large number of recommendations; not every single one of them is strictly necessary to prevent problems, but none of them will 'hurt' the functioning of an MBS. As for the programming overhead caused by this document, there is at least one example of an echo server (Echoput) that implements the full set of recommendations; the size of the (perl) code fits on two pages.

In addition to the rules that should protect against loops and explosions, there are also some recommendations reflecting common sense. For instance, if a user sends a message flagged 'urgent' to a mail based file server, he would not only expect his request message to be handled with extra priority, but also the reply message.

Protocols

Depending on the implementation of the MBS, different recommendations may be used. E.g. A P1 MBS cannot follow all recommendations for RFC 822 based MBSs and vice versa.

For the reader's convenience, the requirements that are applicable to different MBS implementations are explicitly stated in the different terminologies. The requirements are labelled as follows:

#RFC#	Applies to RFC 822 on top of RFC 821 (SMTP) based MBSs
#821#	Applies to RFC 821 (SMTP) based MBSs
#822#	Applies to RFC 822 based MBSs
#400#	Applies to X.400 (both 84 and 88) based MBSs
#84#	Applies to X.400(84) based MBSs
#88#	Applies to X.400(88) based MBSs
#P1#	Applies to P1 based MBSs
#P2#	Applies to P2 based MBSs
#P3#	Applies to P3 based MBSs

2. Definitions

Mail Based Server

An MBS is a process that automatically generates one or more messages (the output messages) as a result of receiving a message (the input message). An MBS can be modelled and/or implemented in one of the following ways:

- #RFC#: As a process sitting directly on top of SMTP. This is called an 821 MBS. If, in addition, the MBS is RFC 822 based, it is called an 822 MBS.

- #400#: within the MTS, in which case it can be considered an enhancement of the X.400 message dispatcher. This is called a P1 MBS.

- #400#: as an MTS service user, in which case it can be considered an automated User Agent (UA). Per default, this is called a P3 MBS. If, in addition, the MBS is P2 based, it is called a P2 MBS. P7 based MBSs are not considered in this document.

The number of output messages and its contents depend on the kind of server and on the contents of the input message.

Dedicated and non-dedicated MBSs

A dedicated MBS is an MBS that is meant to be used as an MBS only. Examples of non-dedicated MBSs are temporarily auto-forwarding user agents (UAs), and UAs that automatically send back vacation notes (auto-repliers). Although software developers are encouraged to implement such features as if it concerned a dedicated MBS, there are some substantial differences between the two types, the main one being that it is not realistic to assume a separate MBS administrator (see below) for every stand-alone UA.

MBS administrator

For every dedicated MBS, there exists an MBS administrator who is responsible for managing the MBS.

Input- and output messages

An input message is a message that triggers the generation of (a) message(s) by an MBS.

An output message is a message that is being generated by an MBS as a result of a received input message.

If an MBS encounters an exceptional situation (as defined in the recommendations below), one exception output message is generated instead of a regular output message. If a non-dedicated MBS does not have an MBS administrator, the exception output message may either be sent to the originator (see below) of the input message instead, or no output message may be generated at all.

MBS Submit Permission

Associated with an MBS is a number of addresses that are allowed to use the MBS (I.e. have the MBS send output messages). Implementation of MBS Submit Permission is considered a local matter. The main implementation options are:

- Implicit: Only those addresses explicitly listed are not allowed to send messages to the MBS.

- Explicit: Only those addresses explicitly listed are allowed to send messages to the MBS.

Message originator

#RFC# The originator of an input message is defined as the value of the Sender: field, or if this attribute is not present, the value of the From: field. For non RFC 822 messages, the originator of an input message is defined as the value on the RFC 821 MAIL FROM: line.

#400# For P2 messages, the originator of an input message is defined as the P2.originator, or if this attribute is not present, the P2.authorizingUsers. For non-P2 messages, the originator of an input message is defined as the P1.originator.

3. Mail based server types

This chapter defines the different types of MBSs. Two main types are identified: repliers and forwarders.

3.1. Repliers

Intuitively speaking, a replier is an MBS that will send an output message to the originator of the input message. There are also exceptions to this rule, such as replying to a Reply-To: field. More formally speaking, a replier is characterised by the fact that the recipient of the output message is uniquely defined in (the heading of) the input message. The different types of repliers can be classified by the number and content of the output message.

Echo server

An echo server is a dedicated replier that will generate exactly one output message, containing the input message.

Mailer demon

This document does not consider the behaviour of X.400 delivery reports and notifications, which is assumed to be well defined in X.400 already. RFC 822 mailers and RFC 1327 gateways however can generate a message explaining the (NON-)Delivery of an input message. In this case the mailer/gateway is acting as an MBS.

For mailer demons, the MBS administrator is the administrator of the mailer/gateway.

Command server

The contents of an output message submitted by a command server depend on commands that were included in the input message. Concrete examples are file servers, e-mail archie servers, DL-registration servers and address conversion servers.

Although it is beyond the scope of this document to define detailed requirements for the command syntax used by command servers, some general recommendations concerning header fields are made in this document.

Auto-replier

Some UAs have an auto-reply feature that will temporarily and/or conditionally turn the UA into an MBS. Thus an auto-replier is a non-dedicated replier. The content of the output message is often a note such as 'I am on holidays.' An auto-replier has a certain lifetime, which is defined as the time span between switching the auto-replier on and back off again.

3.2. Forwarders

A forwarder is an MBS that will send its output messages to a list of recipients. These recipients are independent of (the heading of) the input message.

Distribution List

Upon receiving an input message, a DL will generate output messages to a list of DL members, which is managed by the DL administrator.

At the moment many vendor-specific implementations of DLs exist, some of which are nothing more than local multi-recipient aliases, others use local directories for DL expansion. This document defines the requirements for DLs as well as implementation options.

A moderated DL is modelled as a normal DL with an extra filtering of the input messages by a human. In case of message rejection by the moderator, it is considered good manners for the moderator to follow the recommendations that this document describes for mailer demons. If the message is accepted for distribution, the moderator will transparently pass through all MBS control information (headers) to the actual DL. The moderation process itself is considered a local matter.

Auto-forwarder

Some UAs have an auto-forward feature that will temporarily and/or conditionally turn the UA into an MBS. Thus an auto-forwarder can be considered a non-dedicated forwarder. Upon receiving an input message, an auto-forwarder will submit an output message to a locally defined (list of) address(es), which is managed by the owner of the UA. Although an auto-forwarder often has a certain lifetime, like an auto-replier, this has no implications for the requirements for auto-forwarders.

4. Recommendations

Depending on the implementation, MBSs follow the requirements defined in RFC 822, RFC 821, X.411 and/or X.420 as a minimum.

This document describes additional requirements in terms of RFC 821, RFC 822, P1, P3, and P2. Note that some RFC 822 recommendations deal with non-standard headers described in RFC 1327. This is needed to provide protection across gateways.

The following table lists the recommendations for the MBS types distinguished above. The key to the symbols is self-explanatory. The last column states, for each recommendation, which MBS implementations are affected.

Key to symbols in table 1:

+	Recommended
s	Suggested
o	Optional
d	Don't care
n/a	Not applicable
.	Depends on other factors
-	Not recommended

	auto-answ.	comm. serv.	mail. demon	echo serv.	auto-forw.	dist. list	protocols
AR1.1	+	+	+	+	.	.	P2
AR1.2	+	+	+	+	.	.	822 P2
AR1.3	+	+	+	+	.	.	822 P2
AR1.4	+	+	+	+	.	.	88.P1 88.P3
AR1.5	+	d	+	d	d	.	822 P2
AR2	+	+	+	+	+	.	all
AR3	o	+	-	+	n/a	n/a	822 P2
AR4	o	+	-	+	n/a	n/a	822 P2
AR5	o	+	.	+	n/a	n/a	822 P2
AV1	o	+	-	+	.	.	822 P2
AV2	s	+	+	+	.	.	all
AV3	+	+	+	+	n/a	n/a	822 P2
AV4	+	+	+	+	n/a	n/a	822 P2
AV5	o	+	+	+	.	.	821 P1 P3
AV6	o	+	+	+	.	.	822 P2
AV7	+	+	+	+	.	.	P1 P3
AV8	+	+	+	+	.	.	P2
AV9	s	s	o	+	-	-	822 P2
AV10	-	-	-	-	s	-	822 P2
AV11	.	.	+	.	n/a	n/a	821 P1 P3
AV12	.	.	+	.	n/a	n/a	822 P2
AV13	+	+	+	+	+	+	P1
AV14	-	-	-	-	+	-	822 P2
AC1	+	+	+	+	+	+	822 P2
AC2	+	+	+	+	+	+	822 P2
AC3	+	+	+	+	+	+	822 P1 P3
AC4	.	.	.	s	+	+	P1 P3
AC5	-	-	-	-	-	+	P1 P3
AD1	+	+	+	+	+	+	all
AD2	o	-	+	-	o	-	all
AD3	n/a	n/a	n/a	+	n/a	n/a	all
AD4	n/a	s	n/a	s	n/a	n/a	all
AD5	n/a	n/a	+	n/a	n/a	n/a	all
AD6	n/a	n/a	n/a	n/a	n/a	s	all
B1	-	o	s	+	-	-	822 P2
B2	o	o	o	o	-	o	822 P2
B3	n/a	+	n/a	n/a	n/a	n/a	822 P2
B4	n/a	+	n/a	n/a	n/a	n/a	822 P2
B5	-	-	-	-	+	-	P2
E1	+	+	+	+	+	+	822 P2
E2	+	+	+	+	+	+	all
I1	n/a	s	n/a	s	n/a	s	all
I2	o	+	+	+	o	o	all
I3	s	n/a	n/a	n/a	n/a	n/a	all
I4	n/a	n/a	n/a	n/a	n/a	s	n/a

Table 1. Table of recommendations

4.1. Attribute/header restrictions (AR)

AR1

The following attributes will not be used in the output message:

AR1.1

#P2# Recipient.replyRequest (i.e. should equal FALSE, as per default)

AR1.2

```
#84#P2#         replyBy
#88#P2#         reply-time
#822#           Reply-By:
```

AR1.3

```
#84#P2#         expiryDate
#88#P2#         expiry-time
#822#           Expiry-Date:
```

AR1.4

```
#88#P1#P3#      Proof-of-delivery-request
```

the value of this argument defaults to proof-of-delivery-not-requested.

AR1.5

```
#84#P2# replyToUsers
#88#P2# reply-recipients
#822# Reply-To:
```

AR2

An auto-forwarded message is not valid as an input message. The result is the generation of an exception output message.

AR3

If the following field is present in the input message, the output message will be sent to this address. Otherwise the output message will be sent to the originator of the input message. If the following field contains more than one address, an output message is at least sent to the first address of this filed. Sending to the others is not recommended.

```
#84#P2# replyToUsers
#88#P2# reply-recipients
```

#822# Reply-To:

AR4

#822# If an output message is not sent to the originator of the input message, its From: field field will contain the addresses of the From: and the Sender: fields of the input message. In this case the Sender: field of the output message contains the address of the MBS administrator.

#P2# If an output message is not sent to the P2.originator of the input message, its P2.authorizingUsers field will contain the addresses of the P2.originator and the P2.authorizingUsers of the input message.

AR5

Echo servers will send an exception output message if the input message contains either of the following attributes:

```
#822#     In-Reply-To:
          References:

#P2#      In-Reply-To
          crossReferences
```

4.2. Attribute/header values (AV)

AV1

If the following field is used in the output message, it will not contain the address of the MBS.

#84#P2# replyToUsers
#88#P2# reply-recipients
#822# Reply-To:

AV2

Repliers will not send output messages to addresses which are likely to be MBSs, such as addresses with the following values in the local address designator (S, CN, localpart):

autoanswer
echo
listserv
mailerdaemon
mirror
netserv
server

These values must be matched in any combination of upper case and lower case. Instead, an exception output message is generated. This list is subject to change; an up-to-date version of this list is available in [Noreply]

AV3

The following attribute of the output message will have the following value

#84#P2# inReplyTo : IPMessageID of input message
#88#P2# replied-to-IPM : this-IPM of input message
#822# In-Reply-To: : Message-ID of input message

AV4

The following attributes are optional in an output message. If used, they will contain the following value

#84#P2# crossReferences : IPMessageID of input message
#88#P2# related-IPMs : this-IPM of input message
#822# References: : Message-ID of input message

AV5

#P1#P3# The P1.originator of the output message contains the address of the MBS administrator.

#821# The MAIL FROM: line of the output message contains the address of the MBS administrator.

AV6

#P2# The P2.originator of the output message contains the address of the MBS administrator.

#822# The From: field of the output message contains the address of the MBS administrator.

AV7

#84#P1#P3# Every PerRececipientFlag in the output message will have the following bits set:

Report Request:	01
User Report Request:	00

i.e. the Non-delivery Notification service will be prevented.

AV8

The following argument will be empty in the output message:

#84#P2# Recipient.reportRequest
#88#P2# NotificationRequests

AV9

The following attribute of the output message will contain the string 'Re: ', concatenated with the subject of the input message.

#822# Subject:
#P2# subject

AV10

The following attribute of the output message will contain the subject of the input message, concatenated with the string '(for)'.

#822# Subject:
#P2# subject

AV11

#P1#P3# The P1.recipient of a (non-)DM equals the P1.originator of the input message.

#821# The RCPT TO: field of a (non-)DM equals the MAIL FROM: of the input message.

AV12

#P2# The P2.recipient of a (non-)DM equals the P1.originator of the input message.

#822# The To: field of a (non-)DM equals the originator of the input message.

AV13

#P1# All P1.ExtensionIdentifiers in an output message will be distinct.

AV14

#P2# The output message(s) will have the P2.autoForwarded flag set to true.

4.3. Attribute/header conservation (AC)

The following attributes will have the same value in the output message as in the input message

AC1

In order to propagate the originator's request for privacy to the output message(s):

#822#	Sensitivity:
#P2#	P2.sensitivity

AC2

#822#	Importance:
#P2#	Importance

AC3

#822#	Priority:
#P1#P3#	Priority

AC4

#84#P1#P3#	ContentType

AC5

#P1#P3#	contents

4.4. Addresses (AD)

Please note that all recommendations for names of MBSs and MBS administrators concern internationally used MBSs. Local MBSs can use similar mechanisms in their local language.

AD1

The address of the MBS administrator will be the same as that of the MBS, except for the

#RFC# localpart
#400# Personal Name

AD2

The MBS administrator of a mailer demon has an address with the following local address designation:

AD3

The following attribute of the echo server address will have the value "echo".

#RFC# localpart
#400# Personal Name

AD4

The following attribute in the address of the administrator of a dedicated replier is that of the replier, concatenated with "-reply".

#RFC# localpart
#400# Surname

AD5

A message addressed to an address with the following local address designation will always result in an NRN or a non-DM being generated.

#RFC# localpart = nosuchuser
#84# Surname=nosuchuser
#88# Surname=nosuchuser ; CN=nosuchuser

AD6

The following attribute in the address of the administrator of a dedicated replier is that of the replier, concatenated with "-request".

#RFC# localpart
#400# Surname

4.5. Body (B)

B1

The complete input message (including headers) will be included in the output message in a readable format, e.g. in IA5Text or ASCII.

B2

Additional information is included in separate bodyparts of the output message.

B3

Commands will only be put in the body of the input message, e.g. a command server will ignore the following field.

#822# Subject:
#P2# subject

B4

The recipient of the output message can be uniquely identified from the heading of the input message. I.e. Alternate recipients will not be negotiated in the body of the input message. This will ensure that the recipients can still be uniquely identified after the input message has traversed a protocol gateway.

B5

#P2# The input message will be encoded as a P2.ForwardedIPMessage bodypart in the output message.

4.6. Exceptions (E)

E1

In case of an MBS Submit Permission violation

#822#P2# a non delivery message will be sent to the originator of the input message. The non delivery message will have the following text in the message body:

"Originator not allowed to send to this address"

#84#P1# a P1.DeliveryReportMPDU will be sent to the P1.originator of the input message. The P1.DeliveryReportMPDU will have the following values:

ReasonCode:	unableToTransfer(1)
DiagnosticCode:	uaUnavailable(4)
SupplementaryInformation:	"Originator not allowed to send to this address"

E2

Only the types of input messages listed below are valid as input messages. Any other type of input message (reports, receipt notifications) will lead to the generation of an exception output message.

#84#P1# UserMPDU
#84#P2# IM-UAPDU
#88#P1# Message
#88#P2# IPM
#822# No restrictions

#400# P1.Probes are expected to be handled by the MTS and are thus not interpreted by the MBS itself.

4.7. Implementation options (I)

I1

MBS Submit Permission implementation will be 'implicit'. This means that MBSs that have not explicitly implemented this function can still claim to be implicitly open to anyone.

I2

The MBS logs the originator of the input message and the recipient(s) of the output message(s) so that the MBS administrator can track down malicious behaviour. Any further logging is optional.

I3

Auto-repliers will at least log the originator of the input message. During the lifetime of an auto-replier, at most one output message per input message originator is generated.

I4

#P2# Even if a DL is used for distribution of P2 messages, it is still recommended to implement it within the MTS, i.e. as P1 MBSs. This has some important advantages over P3/P2 based implementations (see also [SHK 92]):

- Using P3 would result in loosing P1.TraceInformation
- Better alignment with X.400(88), which also defines DLs within the MTS
- An MTS DL distributes P1.UMPDUContent transparently, and will thus implicitly implement one of the requirements for DLs.

5. Implementations

There are a number of MBS implementations that follow most of the recommendations listed in this document. They include:

Echoput	(echo server)
AUSSIE	(echo server)
Concord	(echo server, DLs)
Squirrel	(command server)
EAN	(DLs, auto-forwarding, auto-answer, echo)
PP	(DLs, auto-answer, echo)

6. Acknowledgements

Within the context of the connectivity testing tool 'concord', initial work on the requirements for echo servers and distribution lists was done within COSINE MHS and XNREN ([Concord]).

Thanks for ideas, comments, flames and corrections: Allen Cargille (XNREN), Harald Alvestrand (SINTEF), Urs Eppenberger (SWITCH), Paul Klarenberg (NetConsult), Ignacio Martinez (redIRIS), Juan Pizzorno (DFN), Eric Thomas (SUNET), Johan Vromans (Multihouse).

7. Bibliography

821 Jonathan B. Postel, "Simple Mail Transfer Protocol", RFC 821, University of Southern California, August 1982

822 Crocker, D., "Standard of the Format of ARPA Internet Text Messages", RFC 822, UDEL, August 1982.

1211 Westine, A. & Postel, J., "Problems with the Maintenance of Large Mailing Lists", RFC 1211, March 1991.

1327 Hardcastle-Kille, S., "Mapping between X.400(1988) / ISO 10021 and RFC 822", RFC 1327, UCL, May 1992.

1328 Hardcastle-Kille, S., "X.400 1988 to 1984 downgrading", RFC 1328, UCL, May 1992

Concord J. Houttuin, "Concord functional requirements", COSINE MHS server, Mail: cosine-mhs-server@nic.switch.ch, FTP: nic.switch.ch, Username: cosine , File: procedures/echo-server-reqs

Noreply "list of surnames/usernames not to automatically reply to", COSINE MHS server, Mail: cosine-mhs-server@nic.switch.ch, FTP: nic.switch.ch, Username: cosine , File: procedures/dontreply

X.4xx(84) CCITT Recommendations X.400 - X.430. Data Communication Networks: Message Handling Systems. CCITT Red Book, Vol. VIII - Fasc. VIII.7, Malaga-Torremolinos 1984

X.4xx(88) CCITT Recommendations X.400 - X.420. Data Communication Networks: Message Handling Systems. CCITT Blue Book, Vol. VIII - Fasc. VIII.7, Melbourne 1988

SHK92 Hardcastle-Kille, S., "MHS use of the Directory to support distribution lists", Internet-Draft draft-ietf-mhsds-mhsuse-02.txt, November 1992

8. Abbreviations

ASCII	American Standard Code for Information Exchange
CCITT	Comite Consultatif International de Telegraphique et Telephonique
COSINE	Co-operation for OSI networking in Europe
DL	Distribution List
DM	Deliver Message
EAN	MHS software (not an abbreviation)
IPM	Inter-Personal Message
IPN	Inter-Personal Notification
ISO	International Organisation for Standardisation
MHS	Message Handling System
MBS	Mail based server
MOTIS	Message-Oriented Text Interchange Systems
MTA	Message Transfer Agent
MTL	Message Transfer Layer
MTS	Message Transfer System
NJE	Network Job Entry
NRN	Non-Receipt Notification
PP	MHS software (not an abbreviation)
RARE	Reseaux Associes pour la Recherche Europeenne
RN	Receipt Notification
SMTP	simple mail transfer protocol
UA	User Agent

9. Author's Address

Jeroen Houttuin

RARE Secretariat
Singel 466-468
NL-1017 AW Amsterdam
Europe
Tel +31 20 6391131
Fax +31 20 6393289
houttuin@rare.nl