ETSI TS 102 233 V1.1.1 (2004-02)

Technical Specification

Telecommunications security;
Lawful Interception (LI);
Service specific details for E-mail services

Reference

DTS/LI-00003

Keywords

email, handover, interface, IP, lawful interception,
security, traffic

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Lawful Interception (LI).

Introduction

The present document describes what information is required for the handover of intercepted IP-based E-mail traffic from a CSP to an LEMF. The present document covers a stage 2 description of the data, but does not specify any functionality within the scope of TS 102 232 [3].

The ITU-T Recommendation I.130 [6] method for characterizing a service will be used as a general framework for the present document. The modified concept of a "stage 1" will be called the "attributes" of the interface. The attributes of the interface are the sum total of all the constituent attributes that an interface may need to communicate. The modified concept of a "stage 2" will be called the "events" of the interface. The events of the interface define the rules of the relationships between the attributes that are required to arrange the disjoint attributes into meaningful information for an E-mail service interaction.

The present document is intended to be general enough to be used in a variety of E-mail services. It should be recognized that a side effect of this approach is some IRI fields identified may be difficult to extract or non-existent depending on the E-mail service being intercepted. In such cases it may be completely reasonable that the delivered IRI contain empty fields or fields with the value 0.

1 Scope

The present document contains a stage 1 like description of the interception information in relation to the process of sending and receiving E-mail. The present document also contains a stage 2 like description of when IRI and CC shall be sent, and what information it shall contain.

It is recognized that "Instant Messenger" and "Chat" applications are another way of exchanging electronic text messages. While the present document may be applicable to such applications it is in no way a goal of the present document to address these methods of electronic text messaging.

The definition of handover transport and encoding of HI2 and HI3 is outside the scope of the present document. Refer to TS 102 232 [3].

The present document is designed to be used where appropriate in conjunction with other deliverables that define the service specific IRI data formats. The present document aligns with TS 133 108 [5], ES 201 671 [4], TS 101 331 [1] and TR 101 944 [2].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI TS 101 331: "Telecommunications security; Lawful Interception (LI); Requirements of law enforcement agencies".

[2] ETSI TR 101 944: "Telecommunications security; Lawful Interception (LI); Issues on IP Interception".

[3] ETSI TS 102 232: "Telecommunications security; Lawful Interception (LI); Handover specification for IP delivery".

[4] ETSI ES 201 671: "Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

[5] ETSI TS 133 108: "Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) (3GPP TS 33.108 version 5.5.0 Release 5)".

[6] ITU-T Recommendation I.130: "Method for the characterization of telecommunication services Supported by an ISDN and network capabilities of an ISDN".

[7] IETF RFC 0822: "Standard for the format of ARPA Internet text messages".

[8] IETF RFC 1939: "Post Office Protocol - Version 3".

[9] IETF RFC 2821: "Simple Mail Transfer Protocol".

[10] IETF RFC 3501: "Internet Message Access Protocol - Version 4 rev1".

[11] ITU-T Recommendation X.680/ISO/IEC 8824-1: "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

E-mail Address: ARPANET E-mail address

NOTE: As described in RFC 0822 [7], clause 6.

IMAP4: protocol used to manipulate mailbox parameters on a server

NOTE: Described in RFC 3501 [10].

mailbox: destination point of E-mail messages

POP3: widely used protocol for downloading E-mails from a server to a client

NOTE: Described in RFC 1939 [8].

recipient: E-mail address of a destination mailbox for an E-mail being transmitted

NOTE 1: Each E-mail may contain one or more recipients.

NOTE 2: In this definition there is no distinction made between E-mail addresses on a "To:" line and E-mail addresses on a "Cc:" or "Bcc:" line. They are all "recipients" of the E-mail.

sender: E-mail address of the mailbox that originated an E-mail being transmitted

NOTE: Each E-mail contains only one sender.

SMTP: widely used protocol for transferring E-mails between computers

NOTE: described in RFC 2821 [9].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

APOP	POP3 authentication message
ASN.1	Abstract Syntax Notation 1
CC	Content of Communication
CPE	Customer Premises Equipment
CSP	Communications Service Provider
HTTP	Hyper Text Transfer Protocol
IMAP4	Internet Message Access Protocol version 4
IP	Internet Protocol
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
MTA	Mail Transfer Agents
NWO	Network Operator
POP3	Post-Office Protocol version 3
PSTN	Public Switched Telecommunication Network
RETR	POP3 Retrieve message
SMTP	Simple Mail Transfer Protocol
SP	Service Provider
TCP	Transmission Control Protocol

4 General

4.1 E-mail services

E-mail services are those services which offer the capability to transmit or receive ARPANET text messages. The following description is taken from RFC 0822 [7]:

"In this context, messages are viewed as having an envelope and contents. The envelope contains whatever information is needed to accomplish transmission and delivery. The contents compose the object to be delivered to the recipient".

E-mail service, in general, can be divided into two categories: those services which allow a computer to transfer a message to another computer; and those services which allow users to manipulate their mailbox by doing such things as downloading messages from the mailbox and deleting messages from the mailbox. Both of these categories of E-mail services can be of interest to LEAs and are therefore within the scope of the present document.

NOTE: When using IP-packet delivery, control level packets that are associated with the targeted E-mail may be delivered as content. Control level packets are those packets that are used by the E-mail transfer protocol to setup the E-mail communication and to terminate the E-mail communication and are outside of the traditional RFC 0822 [7] formatted E-mail. This allows for different interception solutions without burdening the MF with the responsibility of "cleaning" up said differences in input.

5 System model

5.1 Reference network topology

The network topology shown in figure 1 is intended to represent the many relationships that may exist between the entities involved in E-mail communications. Actual scenarios using this diagram are enumerated in clause 5.2. The following should be considered when viewing figure 1:

- The term "Mail Server" is used to represent a logical entity that relays mail for its mail clients, receives and (temporarily) stores mail for its mail clients, and allows mail clients access to the aforementioned stored mail and the ability to delete it from the mail server.
- The term "Mail Client" is used to represent a logical entity that either injects mail into the network, removes mail from the network or reads mail from the network.
- Mail Client and Mail Server numbers are used to indicate what entities share a client-server relationship, so Mail Client1 is a client of Mail Server1, etc.
- A Mail Server may communicate with any other Mail Server within figure 1.

NOTE: Web access to mail is commonly used; web mail is addressed in annex H.

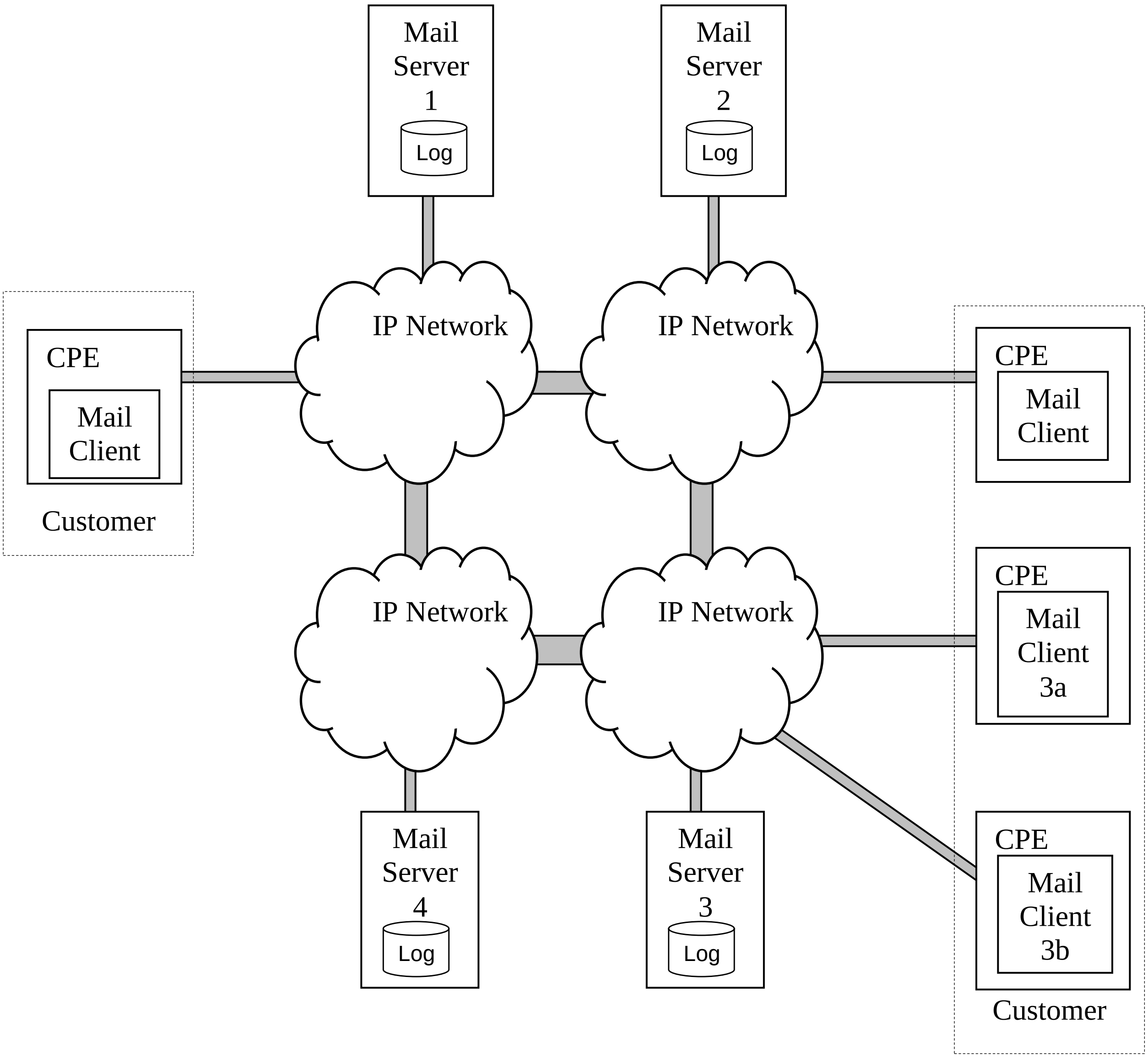

Figure 1: Reference network topology

5.2 Reference scenarios

5.2.1 E-mail send failure

It may occur that E-mails sent into the Internet do not reach their intended target. The most common reason for this would seem to be a mistaken E-mail address, but could also be problems contacting the receiving mail server or other server issues. Note that a failure reply message is not always generated and if a failure reply message is generated, it is generated by the Mail Server that first experiences problems transferring the mail message.

a) Client3a sends an E-mail to nobody@MailServer4.com and gives the E-mail to the clients' server, Mail Server3.

b) Mail Server3 fills in part of the E-mail envelope and routes the E-mail to Mail Server4.

c) Mail Server4 replies to Mail Server3 that the recipient is unknown.

d) Mail Server3 creates a "reply" message to Mail Client3a stating that the recipient was unknown, and either pushes that message to the client or stores it in the clients' mailbox for later retrieval.

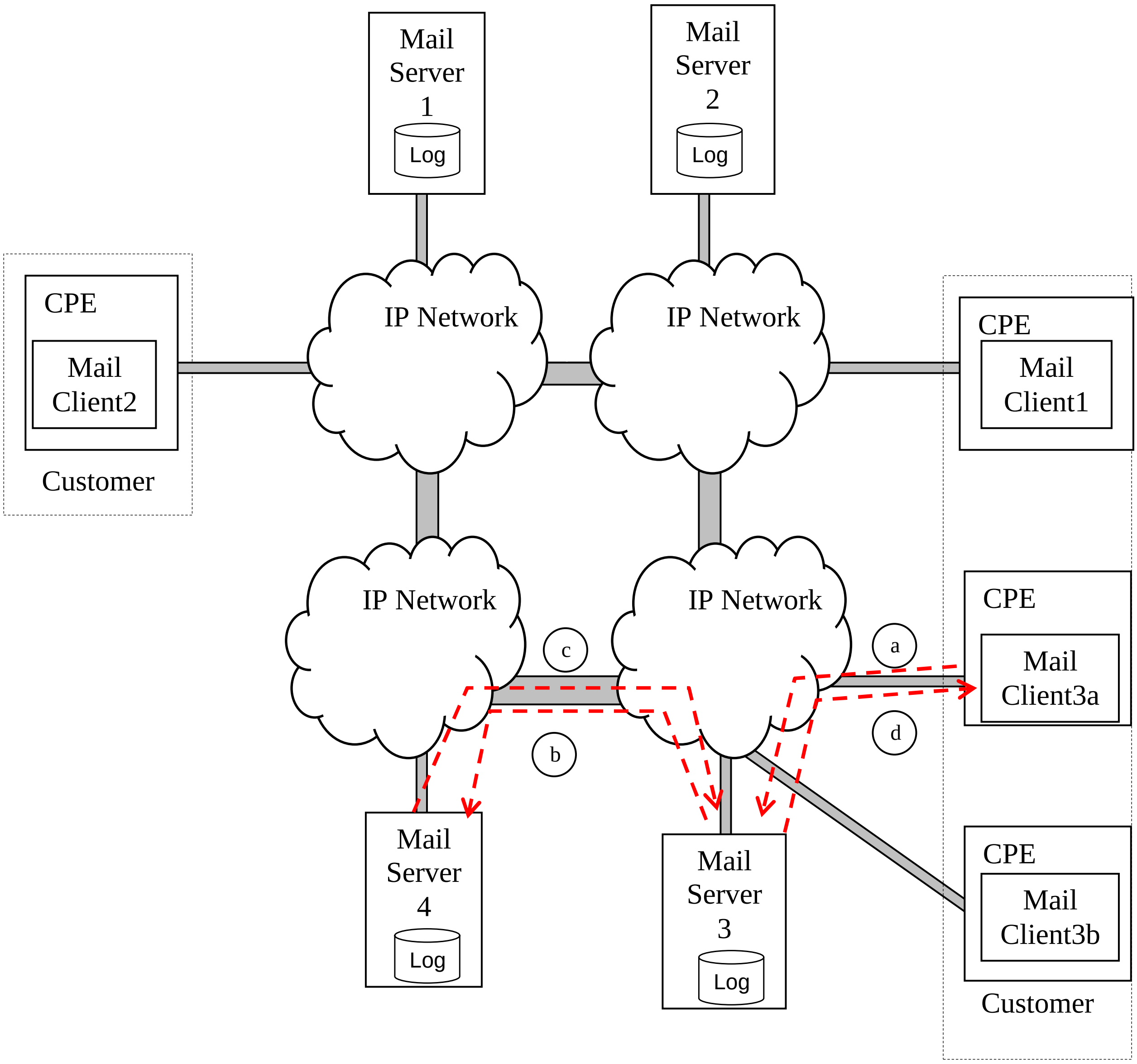

Figure 2: E-mail send failure

5.2.2 E-mail send success

This scenario represents what is likely to be the most common case of an E-mail send. While it is unclear how many E-mails go directly from a clients E-mail server to the destination E-mail server, it is clear that routing of E-mails through Mail Transfer Agents (MTA) is not uncommon and as such is the scenario represented here. The direct routing scenario is a subset where the middle mail server is removed. Note also that the client sending the E-mail is not on the same administrative network as its mail server.

a) Client1 sends an E-mail to client3b@MailServer3.com and gives the E-mail to the clients' server, Mail Server1.

b) Mail Server1 fills in part of the E-mail envelope and forwards the mail to Mail Server4 for forwarding.

c) Mail Server4 attaches its information to the E-mail envelope and forwards the mail to Mail Server3.

d) Mail Server3 either pushes the message to the Mail Client3b or stores it in the clients' mailbox for later retrieval.

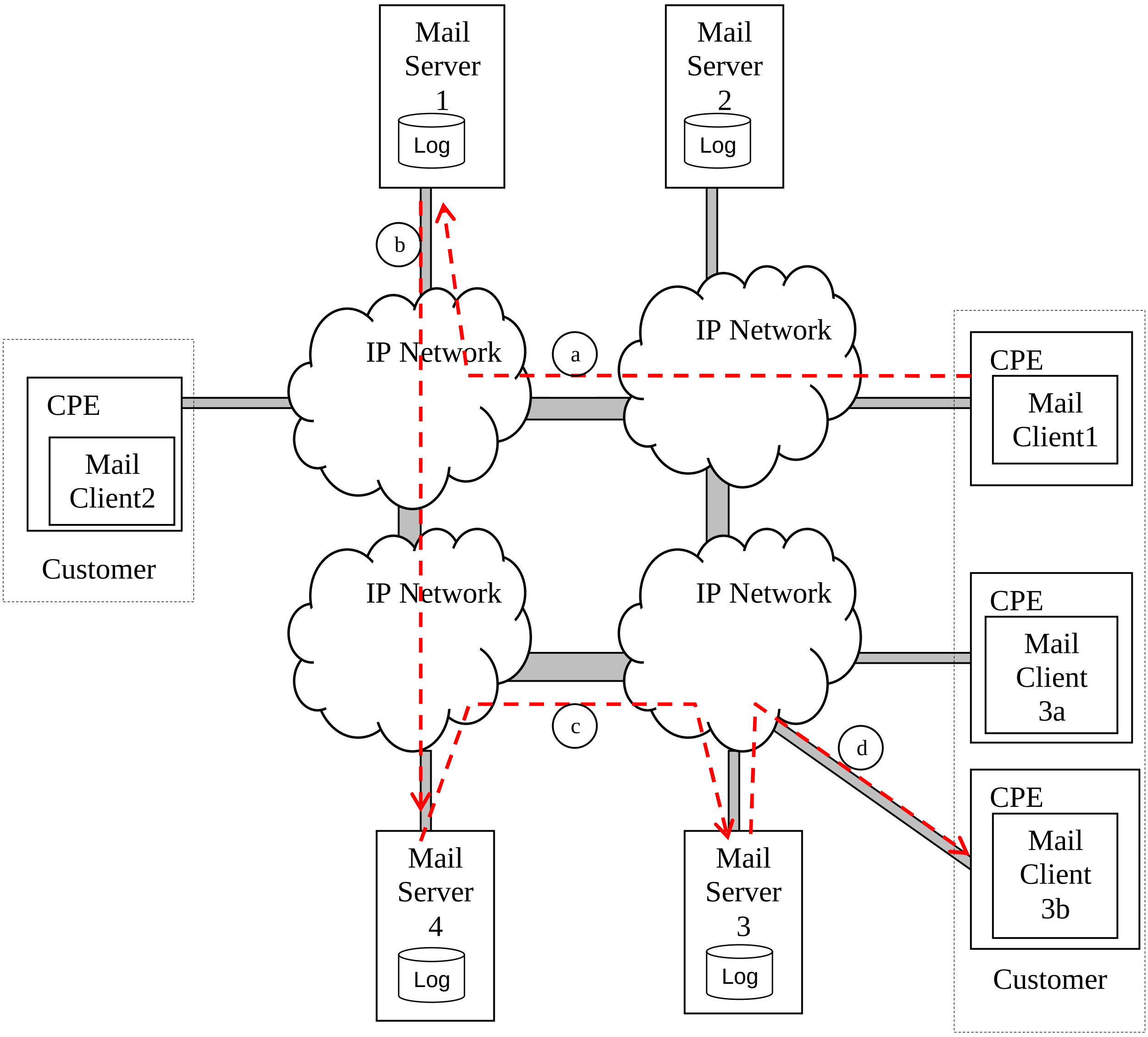

Figure 3: E-mail send success

5.2.3 E-mail download detail

This scenario enumerates the processes that must take place in any E-mail download process. It is assumed that some set of E-mail is already resident on the Mail Server3 in the mailbox for Mail Client3a.

a) Mail Client3a sends login credentials. This may take several messages or may be accomplished in a single message depending on the mailbox access protocol. What is protocol invariant is that this login process will contain some form of authentication process.

b) Mail Server3 sends an "authentication success" message to indicate to the client that the login process is complete. At this stage Mail Server3 may push down mailbox state to the client, or may wait for the client to request mailbox state. Using POP3, however, Mail Server3 will not push down messages until the have been explicitly requested by the client.

c) Mail Client3a may request a message or a set of messages to be downloaded, however this step may be bypassed in some protocols.

d) Mail Server3 downloads the requested messages to Mail Client3a.

e) After the mail has been downloaded the server may delete the message as the result of a request.

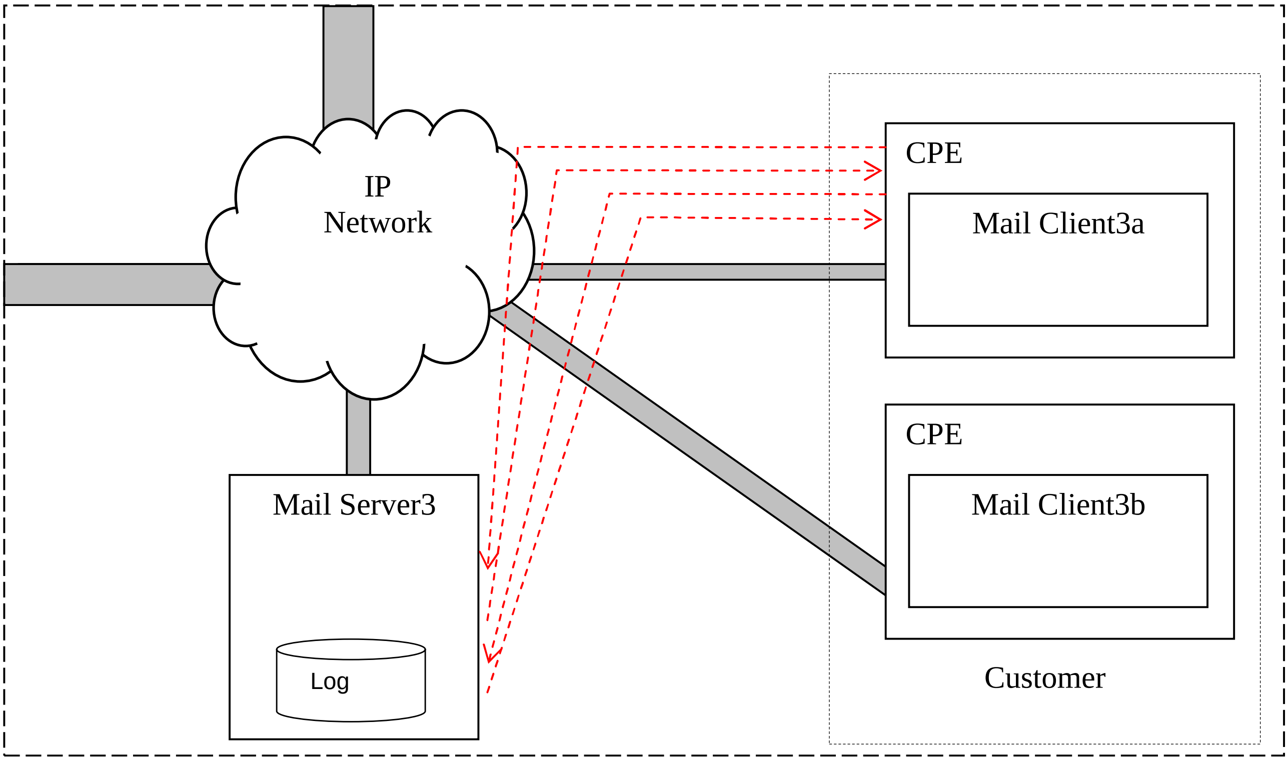

Figure 4: E-mail download detail

5.2.4 E-mail send detail

This scenario enumerates the processes that must take place in any E-mail send process. In the scenario the relationship between Mail Server3 and Mail Client3a is such that the mail is first sent to Mail Server3, which then forwards the mail. While this process seems universally true it need not be true. Mail Client 3a could send the mail to the terminating mail server.

a) Mail Client3a sends introduction. This may take several messages or may be accomplished in a single message depending on the mailbox access protocol. The authentication features and capabilities is protocol dependent and authentication may be used in some protocols and not in others.

b) Mail Server3 sends a "login success" message to indicate to the client that the login process is complete.

c) Mail Client3a initiates a send by including the sender E-mail address, the list of recipient E-mail addresses, and the text body of the message.

d) Mail Server3 sends a response indicating that the mail has been successfully received. At this point Mail Server3 begins the process of determining the correct mail servers for each of the recipients, updating the mail text to include information in the envelope, and forwarding the mail.

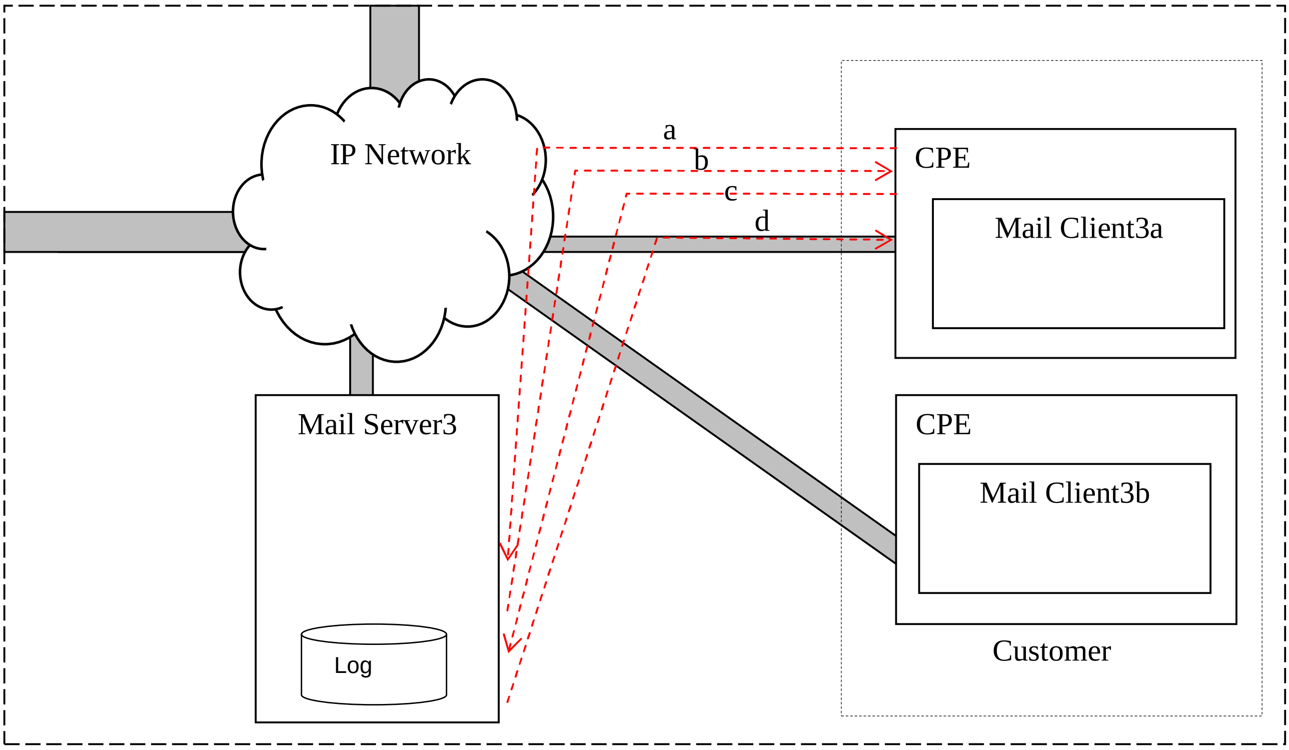

Figure 5: E-mail send detail

6 E-mail events

6.1 Introduction

This clause contains the high level definition of the content and the IRI messages associated with different E-mail communication "events". An "E-mail communication event" is a way of expressing different points in an E-mail transfer where a target may become active. All E-mail communication events are represented by one or more IRI records and potentially content. Clause 6 does not specify how the information is encoded but specifies what information shall be encoded.

This clause only lays out which fields shall be present in each event and what requirement is fulfilled by the field. The definition of each field is either in another document or in clause 7.

6.2 E-mail send event

6.2.1 Introduction

The E-mail send event is represented in clauses 5.2.2 and 5.2.4. This event is represented by a set of IRI and content associated with an E-mail being sent by a target. Each E-mail sent during a session between an E-mail client and an E-mail server must be considered a separate E-mail send event.

There is currently no IRI specified specifically for E-mail send "attempts", and no indication of E-mail send "success" or "failure". E-mail failures often occur a few servers down from where the initial E-mail is sent, and notification of said failure is optional and difficult to automatically correlate when it does occur.

This set of IRI fulfils requirement [E.1.1].

6.2.2 E-mail Send captured content

The target may have been matched for an E-mail send by the E-mail address of the sender, login name of the sender, or the IP address. Due to the wide array of intercept options and possible E-mail protocols the captured content maybe just the equivalent of the RFC 0822 [7] E-mail envelope and text or, at the other extreme, the captured content may be the whole E-mail session. What must be present is the RFC 0822 [7] E-mail envelope and text for E-mails sent by the target.

This clause fulfils requirement [E.2.1] and [E.2.2].

6.2.3 E-mail send IRI

The following information may be present in E-mail Send IRI. The availability of this information will depend on the implementation and national regulations.

Table 1: E-mail send IRI information

Field name	Requirement fulfilled	Where defined
Server IP	[E.1.7]	ES 201 671 [4], IP address
Client IP	[E.1.7]	ES 201 671 [4], IP address
Server Port	[E.1.7]	Clause 7
Client Port	[E.1.7]	Clause 7
E-mail Protocol ID	[E.1.10]	Clause 7
E-mail Sender	[E.1.3]	Clause 7
E-mail Recipient List	[E.1.3]	Clause 7
Total Recipient Count	[E.1.5]	Clause 7
Server Octets Sent	[E.1.7]	Clause 7
Client Octets Sent	[E.1.7]	Clause 7
Message ID	[E.1.12]	Clause 7
Status	[E.1.11]	Clause 7

Note that in this case, both Octets Sent fields are indicators of the amount of communication occurring. Due, however, to differing laws and interception capabilities it is not specified exactly what these byte counts are, only that they accurately represent the amount of information being transferred by the target. That is to say, these byte counts can not be the byte count of an entire E-mail session in which many E-mails are sent but only one of those E-mails was sent by the target entity as the numbers would no longer be representative of the amount of information being transferred by the target. Similarly these byte counts can not be taken to be a one-to-one match of the number of bytes in an E-mail as they may include the control traffic to setup the E-mail or may include some filing system overhead.

Finally it is worth noting that if the intercept capability is not done based on a protocol but instead based on information on a file system, the Server Octets Sent could be 0 if that accurately represents that the server sent little or no information back to the client.

6.3 E-mail receive event

6.3.1 Introduction

The E-mail receive event is best represented in clause 5.2.3 and represents a set of IRI and content associated with an E-mail being received by a target mailbox. Each E-mail received during a session between an E-mail client and an E-mail server must be considered a separate E-mail receive event.

There is currently no IRI defined for E-mail receive "attempts", and no indication of E-mail receive "success" or "failure". The reason for this decision is because it is deemed an excessive burden on all the parties involved in an intercept for the amount of information that can be obtained.

This set of IRI fulfils requirement [E.1.2].

6.3.2 E-mail receive captured content

The target may have been matched for an E-mail receive by the E-mail address of the recipient, login name of the recipient, or the IP address of the client. Due to the wide array of intercept options and possible E-mail protocols the captured content maybe just the equivalent of the RFC 0822 [7] E-mail envelope and text, or, at the other extreme, the captured content may be the whole E-mail session. What must be present is the RFC 0822 [7] E-mail envelope and text for E-mails received by the target.

This clause fulfils requirement [E.2.1] and [E.2.2].

6.3.3 E-mail receive IRI

The following information may be present in E-mail receive IRI. The availability of this information will depend on the implementation and national regulations.

Table 2: E-mail receive IRI information

Field name	Requirement fulfilled	Where defined
Server IP	[E.1.7]	ES 201 671 [4], IP address
Client IP	[E.1.7]	ES 201 671 [4], IP address
Server Port	[E.1.7]	Clause 7
Client Port	[E.1.7]	Clause 7
E-mail Protocol ID	[E.1.10]	Clause 7
E-mail Sender	[E.1.3]	Clause 7
E-mail Recipient List	[E.1.3]	Clause 7
Total Recipient Count	[E.1.5]	Clause 7
Server Octets Sent	[E.1.7]	Clause 7
Client Octets Sent	[E.1.7]	Clause 7
Message ID	[E.1.12]	Clause 7
Status	[E.1.11]	Clause 7

Note that in this case both Octets Sent fields are indicators of the amount of communication occurring. However, due to differing laws and interception capabilities it is not specified exactly what these byte counts are, only that they accurately represent the amount of information being transferred to the target. For instance, these byte counts may not be the byte count of an entire E-mail session in which many E-mails are transferred but only one of those E-mails was destined to the target entity. In that case the session byte count would no longer be representative of the amount of information being transferred to the target. Similarly these byte counts could not be taken to be a one-to-one match of the number of bytes in an E-mail as they may include the control traffic to setup the E-mail or may include some filing system overhead.

Finally it is worth noting that if the intercept capability is not done based on a protocol but instead based on information on a file system, the Client Octets Sent could be 0 if that accurately represents that the client sent little or no information back to the server.

6.4 E-mail download event

6.4.1 Introduction

The E-mail Download Event is best represented in clause 5.2.3 and represents a set of IRI and content associated with an E-mail being downloaded from a target mailbox. Each E-mail downloaded during a session between an E-mail client and an E-mail server must be considered a separate E-mail Download Event.

There is currently no IRI defined for E-mail download "attempts". The reason for this decision is because it is deemed an excessive burden on all the parties involved in an intercept for the amount of information that can be obtained.

This set of IRI fulfils requirement [E.1.2].

6.4.2 E-mail download captured content

The target may have been matched for an E-mail Download by the E-mail address of the recipient, login name of the recipient, or the IP address of the client. Due to the wide array of intercept options and possible E-mail protocols the captured content maybe just the equivalent of the RFC 0822 [7] E-mail envelope and text, or, at the other extreme, the captured content may be the whole E-mail session. What must be present is the RFC 0822 [7] E-mail envelope and text for E-mails received by the target.

This clause fulfils requirement [E.2.1] and [E.2.2].

6.4.3 E-mail download IRI

The following information may be present in E-mail Download IRI. The availability of this information will depend on the implementation and national regulations.

Table 3: E-mail download IRI information

Field name	Requirement fulfilled	Where defined
Server IP	[E.1.7]	ES 201 671 [4], IP address
Client IP	[E.1.7]	ES 201 671 [4], IP address
Server Port	[E.1.7]	Clause 7
Client Port	[E.1.7]	Clause 7
E-mail Protocol ID	[E.1.10]	Clause 7
E-mail Sender	[E.1.3]	Clause 7
E-mail Recipient List	[E.1.3]	Clause 7
Total Recipient Count	[E.1.5]	Clause 7
Server Octets Sent	[E.1.7]	Clause 7
Client Octets Sent	[E.1.7]	Clause 7
Message ID	[E.1.12]	Clause 7
Status	[E.1.11]	Clause 7

7 E-mail attributes

The availability of the information described in this clause will depend on the implementation and national regulations.

7.1 E-mail protocol ID

This attribute can be used to identify the E-mail application or protocol that was used at the point of interception to transfer the E-mail. This should identify which appendix should be looked at for encoding rules. A full enumeration of this attribute is provided in annex D, however a brief list should help provide an example for the definition. This attribute shall contain values including, but not limited to:

- SMTP;
- POP3.

7.2 E-mail address

All E-mail address attributes are text strings that indicate an E-mail address in the form that it was intercepted in. E-mail addresses may be fully qualified, however many points of interception will not provide fully qualified E-mail addresses.

The above definition of an E-mail Address fulfils requirement [E.1.4].

7.3 E-mail recipient list

This is a list of one or more E-mail address of the intended recipients of an E-mail. Note that this list may not be complete and only contains those recipient addresses that can be intercepted by the interception equipment. SMTP can be used as an example, where only a proper sub-set of the recipients can be seen within the protocol itself.

NOTE: The amount of information which can be retrieved from the SMTP protocol depends on the choice of where the interception equipment is placed in the network.

7.4 E-mail sender

This is a single E-mail address representing the intercepted address of the sender of a targeted E-mail.

7.5 Total recipient count

This attribute is an integer representing the total number of recipients that the interception equipment noticed, even if all those recipients could not be explicitly enumerated in the E-mail Recipient List.

7.6 Message ID

This attribute is used, when available, to relay a message identifier with a message. Applications which communicate primarily through message ID's may use this attribute to relay this information to the LEMF. When present, this attribute and its exact meanings will be highly dependent on the E-mail application and will be specified in the application specific appendix.

7.7 Status

This attribute identifies the status of the communication with values of UNKNOWN, FAILED, and SUCCESS. SUCCESS should be used to indicate status when it is clear that the message reached its destination. The destination should be thought of as the terminating point of the action.

Table 4: E-mail events and termination points

E-mail Event	Termination Point
E-mail Send	Recipient Mailbox Received
E-mail Download	Download succeeded
E-mail Receive	Recipient Mailbox Received

When the termination point is not understood by the intercept equipment, or the termination point is not monitored by the intercept equipment and the application operation was not determined to be a failure, then the value of UNKNOWN should be used to indicate status.

When the application operation was determined to be a failure (i.e. an error code or some other means) then the value of FAILED should be used to indicate status.

7.8 Server and client port

These attributes identify the Layer 4 port used for communication of the E-mail. How the "server" and the "client" are distinguished is identified in the appendices on a per E-mail application basis.

7.9 Server and client octets sent

These attributes indicate the number of octets sent by the client and sever during the communication of the E-mail. How the "server" and the "client" are distinguished is identified in the appendices on a per E-mail application basis. As specified above, both of the octet sent numbers need only accurately represent the amount of information being transferred and should not be considered exact counts of bytes sent at any particular protocol layer.

Annex A (normative): SMTP

A.1 SMTP introduction

SMTP can generally be viewed as a means for sending E-mail from one computer to another. The computer which sent the E-mail may not be the original source of the E-mail, and the computer which received the E-mail may not be the ultimate destination.

Clause A.2 indicates which events can be expected when an interception point is either SMTP or at an SMTP server.

Clause A.3 indicates which protocol units one could expect to fill the event attributes.

A.2 SMTP HI2 events

A.2.1 E-mail login event

An SMTP login success event should be generated after the SMTP client has sent the SMTP hello message and the SMTP server has responded with a response indicating success as defined in RFC 2821 [9].

An SMTP login failure event should be generated after the SMTP client has sent the SMTP hello message and the SMTP server has responded with a response indicating failure as defined in RFC 2821 [9].

NOTE: SMTP logins are not well authenticated.

A.2.2 E-mail send event

An SMTP send event should be generated after the SMTP client has sent DATA command and the server has responded with a response indicating a successful send as defined in RFC 2821 [9].

No event should be generated on an unsuccessful send (for further study).

A.2.3 E-mail receive event

An SMTP receive event should be generated after the SMTP client has sent DATA command and the server has responded with a response indicating a successful transfer as defined in RFC 2821 [9].

No event should be generated on an unsuccessful receive (for further study).

NOTE: The difference in an E-mail Receive Event and an E-mail Send Event, for SMTP, is a matter of semantics but may have legal ramifications.

A.3 SMTP HI2 attributes

Table A.1 shows the attributes that need to be filled by the events specified in clause A.2 and the protocol data that should be used to fill these attributes.

Table A.1: SMTP E-mail attributes

Server IP	IP Header, Destination IP of HELO or MAIL FROM message
Client IP	IP Header, Source IP of HELO or MAIL FROM message
Server Port	TCP Header, destination port of HELO or MAIL FROM message
Client Port	TCP Header, source port of HELO or MAIL FROM message
E-mail Protocol ID	SMTP
E-mail Sender	E-mail address specified in MAIL FROM message
E-mail Recipient List	Each address should be from a RCPT TO message that has been accepted by the server for this E-mail
Total Recipient Count	Count of the number of RCPT TO messages that received a positive response from the server
Server Octets Sent	Octet count of the number of bytes sent by the server for the duration of the E-mail send operation. Note that the exact process for determining the number of bytes reported will be highly dependent on the interception equipment deployed and so is not specified here. What is important is that one can get a "feel" for the amount of information the server is exchanging with the client
Client Octets Sent	Octet count of the number of bytes sent by the client for the duration of the E-mail send operation. Note that the exact process for determining the number of bytes reported will be highly dependent on the interception equipment deployed and so is not specified here. What is important is that one can get a "feel" for the amount of information contained in the E-mail sent by the client
Message ID	This is the message ID as specified in the RFC 0822 [7] E-mail header attribute "Message-ID"

A.4 SMTP HI2 event-record mapping

Table A.2 shows the events sent are mapped to the HI2 record type that the event will be sent under.

Table A.2: SMTP E-mail event records

SMTP events	Subject	HI2 record
SMTP log on	Client	Begin
SMTP log on attempt	Client	Report
E-mail send successful	Client	Continue/Report
E-mail send unsuccessful	Client	Continue/Report
SMTP log off	Client	End

Annex B (normative): POP3

B.1 POP3 introduction

POP3 can generally be viewed as a means for remotely manipulating E-mail stored on a server in a mailbox. No "send" facility is provided via POP3.

Clause B.2 indicates which events can be expected when an interception point is either POP3 or a POP3 server.

Clause B.3 indicates which protocol units one could expect to fill the event attributes.

B.2 POP3 HI2 events

B.2.1 E-mail login event

A POP3 login success event should be generated after the POP3 client has sent the POP3 password or APOP message and the POP3 server has responded with an OK response indicating success, as defined in RFC 1939 [8].

A POP3 login failure event should be generated after the POP3 client has sent the POP3 password or APOP message and the POP3 server has responded with a ERR response indicating failure, as defined in RFC 1939 [8].

B.2.2 E-mail download event

A POP3 download event should be generated after the POP3 client has sent RETR command and the server has responded the entire E-mail indicating a successful download, as defined in RFC 1939 [8].

No event should be generated on an unsuccessful download (for further study).

B.3 POP3 HI2 attributes

Table B.1 shows the attributes that need to be filled by the events specified in clause B.2 and the protocol data that should be used to fill these attributes.

Table B.1: POP3 E-mail attributes

Server IP	IP Header, Destination IP of password or APOP message
Client IP	IP Header, Source IP of password or APOP message
Server Port	TCP Header, destination port of password or APOP message
Client Port	TCP Header, source port of password or APOP message
E-mail Protocol ID	POP3
E-mail Sender	E-mail address specified in "From:" line in RFC 0822 [7] compliant E-mail message. It should be well understood that this field may be difficult to extract and is not used by the service therefore it may easily be faked
E-mail Recipient List	Only one address will be present here, and it will be the mailbox address used to login
Total Recipient Count	Always one, given the above definition of E-mail Recipient List
Server Octets Sent	Octet count of the number of bytes sent by the server for the duration of the E-mail download operation. Note that the exact process for determining the number of bytes reported will be highly dependent on the interception equipment deployed and so is not specified here. What is important is that one can get a "feel" for the amount of information contained in the E-mail sent by the server
Client Octets Sent	Octet count of the number of bytes sent by the client for the duration of the E-mail download operation. Note that the exact process for determining the number of bytes reported will be highly dependent on the interception equipment deployed and so is not specified here. What is important is that one can get a "feel" for the amount of information contained in the E-mail downloaded by the client. This value may be 0 if that accurately represents the amount of information being sent by the client was little or non-existent
Message ID	This is the message ID as specified in the RFC 0822 [7] E-mail header attribute "Message-ID"

B.4 POP3 HI2 event-record mapping

Table B.2 shows the events sent are mapped to the HI2 record type that the event will be sent under.

Table B.2: POP3 E-mail event records

POP3 event	Subject	HI2 Record
POP3 log on	Client	Begin
E-mail download	Client	Continue/Report
Modifying Supplementary Service	Client	Continue
Forward on incoming mail	Client	Report
Reply on incoming mail	Client	Report
POP3 log off	Client	End

Annex C (normative): IMAP4

C.1 IMAP4 introduction

IMAP4 is for futur study.

Annex D (normative): E-mail ASN.1

The ASN.1 (ITU-T Recommendation X.680 [11]) module that represents the information in the present document and meets all stated requirements is shown below:

```
EmailPDU
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5) email(2)
version1(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
IMPORTS
    IPAddress
        FROM
        HI2Operations;
            -- ETSI ES 201 671

emailIRIObjId RELATIVE-OID  ::= {li-ps(5) email(2) version1(1) iRI(1)}
emailCCObjId RELATIVE-OID   ::= {li-ps(5) email(2) version1(1) cC(2)}
    -- both definitions relative to {itu-t(0) identified-organization(4)
    -- etsi(0) securityDomain(2) lawfulintercept(2)}
```

```
EmailCC             ::= SEQUENCE
    -- EmailCC is the PDU sent for each "piece" of E-mail captured content.
{
    emailCCObjId        [0] RELATIVE-OID,
    email-Format        [1] Email-Format,
    content             [2] OCTET STRING
        -- Network byte order
}
```

```
Email-Format        ::= ENUMERATED
{
    ip-packet       (1),
        -- When this is the email format, the content will contain the bytes of the IP packet from
        -- the IP header through to the end of the IP packet.
        -- Meets requirement E.2.7.
    application     (2)
        –- Only the IP stack Layer 4 payload, (i.e. no IP or TCP headers).
        -- Meets requirement E.2.8.
}
```

```
EmailIRI            ::= SEQUENCE
    -- EmailIRI is the PDU sent for each "piece" of E-mail IRI.
{
    emailIRIObjId           [0] RELATIVE-OID,
    eventType               [1] E-mail-Event,
    client-Address          [2] IPAddress OPTIONAL,
        -- Provided if available
    server-Address          [3] IPAddress OPTIONAL,
        -- Provided if available
    client-Port             [4] INTEGER OPTIONAL,
        -- Provided if available
    server-Port             [5] INTEGER OPTIONAL,
        -- Provided if available
    server-Octets-Sent      [6] INTEGER,
    client-Octets-Sent      [7] INTEGER,
    protocol-ID             [8] E-mail-Protocol,
    e-mail-Sender           [9] UTF8String (SIZE (0..255)),
    e-mail-Recipients       [10] E-mail-Address-List,
    status                  [11] E-mail-Status,
    total-Recipient-Count   [12] INTEGER (0..4294967295) OPTIONAL,
    message-ID              [13] OCTET STRING OPTIONAL,
        –- Network byte order
    nationalParameter       [14] OCTET STRING OPTIONAL,
        -- Completely defined on a national basis, including byte ordering
    ...
}
```

```
E-mail-Status   ::= ENUMERATED
{
    status-unknown          (1),
    operation-failed        (2),
    operation-succeeded     (3)
}
```

```
E-mail-Event    ::= ENUMERATED
{
    e-mail-send         (1),
    e-mail-receive      (2),
    e-mail-download (3)
}
```

```
E-mail-Protocol     ::= ENUMERATED
{
    smtp        (1),
    pop3        (2),
    undefined   (255),
        -- The protocol is not known or not representable by the current enumeration.
    ...
}
```

```
E-mail-Address-List     ::= SEQUENCE (SIZE (0..1023)) OF UTF8String(SIZE (0..255))
```

```
END -- EmailPDU
```

Annex E (informative): E-mail LI requirements

E.1 HI2 requirements

[E.1.1] The HI2 interface shall support the ability to deliver IRI record(s), without delivering the contents of the message, when a target has sent E-mail.

NOTE 1: How an E-mail send is determined and intercepted is outside of the scope of the present document, however, that E-mail was sent and to whom it was sent is interesting to law enforcement. Likewise the information needed to intercept that an E-mail was sent and to whom it was sent can be determined in many ways including, but limited to, well defined interception points, laws, or combinations of IP interception and more conventional intelligence.

[E.1.2] The HI2 interface shall support the ability to deliver IRI record(s), without delivering the contents of the message, when a target has downloaded E-mail.

NOTE 2: How an E-mail receive is determined and intercepted is outside of the scope of the present document, however, that an E-mail was received and from whom it was sent is interesting to law enforcement. Likewise the information needed to intercept that an E-mail was received and from whom it was sent can be determined in many ways including, but limited to, well defined interception points, laws, or combinations of IP interception and more conventional intelligence.

[E.1.3] The HI2 interface shall support the ability to deliver both the sender E-mail address and recipient E-mail addresses of E-mail as part of the "send" and "receive" events.

NOTE 3: Neither sender nor recipient E-mail addresses are required because of differences in national laws or points of interception may not allow this information to be extracted. That being said, because of differences in national laws or points of interception, both of these pieces of information may be available, therefore we must support the ability to transfer both addresses.

[E.1.4] When HI2 is able to deliver an E-mail address, either sender or receiver, the MF shall not be required to modify the address presentation. For example, if no domain name was present at intercept time, for example, the MF is not required to determine the domain name and append it.

NOTE 4: Many reasons for this, including data integrity and cost, can be used.

[E.1.5] The HI2 interface shall support a means of indicating how many recipient addresses could not be sent with the "send" or "receive" events due to limitations.

NOTE 5: The pathological example is an SMTP intercept with a trillion RCPT TO's. Since there is no expectation that the intercept device or the MF have unlimited resources we must recognize that there is the possibility that some resource on some device in the chain may not be able to handle the number of RCPT TO's, and provide for a means to notify the LEA that we hit this condition.

[E.1.6] The RFC 0822 [7] E-mail message envelope fields of dates, source, and destination may be considered IRI. These fields are defined in RFC 0822 [7].

NOTE 6: These fields clearly mark data that is traditionally passed via a control channel, and therefore should be treated as IRI.

[E.1.7] The E-mail HI2 end record shall contain the following information, when present and available from the layer 3 and layer 4 protocols:

- participating server and client addresses;
- participating server and client ports (i.e. TCP port);
- Bytes sent by the server and client.

NOTE 7: This information should be the control information that provides the LEA with an indication of the quantity of communication occurring.

[E.1.8] E-mail HI2 shall be encoded using ASN.1 and BER.

NOTE 8: This makes the data collectors' job easier as there is not separate encoding and does not impose any additional burden on the MF as it will have to extract the requisite information anyway and will have to support BER anyway.

[E.1.9] The HI2 interface shall support the ability to deliver IRI record(s), without delivering the contents of any messages or passwords, when an attempt has been made to log into the target E-mail account. This record shall also contain the results of the logon attempt.

NOTE 9: This has been required by LEA's.

[E.1.10] The HI2 interface shall support a means of indicating what E-mail application service was intercepted.

NOTE 10: This information can be helpful to the LEA for investigative purposes.

[E.1.11] The HI2 interface shall support a means of indicating the success or failure of an E-mail interaction to the degree that such information is available.

[E.1.12] The HI2 interface shall support the ability to deliver the Message-ID.

NOTE 11: The Message-ID supports the identification in E-mail log-files.

E.2 HI3 requirements

[E.2.1] HI3 delivery of E-mail content shall include the entire E-mail message body. See RFC 0822 [7] for a definition of the body.

NOTE 1: Anything less would be incomplete data.

[E.2.2] HI3 delivery of E-mail content shall include the entire E-mail envelope, when applicable. See RFC 0822 [7] for a definition of the envelope.

NOTE 2: The RFC 0822 [7] envelope can be used by collectors to display the E-mail in a meaningful format. Likewise this is the only place that the envelope can be seen in its entirety. The value of the above two is considered worth the cost of potentially duplicating HI2 data.

[E.2.3] All passwords shall be considered content.

NOTE 3: This is a positive way to express "passwords will not go over HI2".

[E.2.4] The RFC 0822 [7] E-mail message body shall be considered content.

NOTE 4: This is a positive way to express "E-mail message bodies will not go over HI2".

[E.2.5] All RFC 0822 [7] E-mail message envelope fields that are declared optional in RFC 0822 [7] shall be considered content.

NOTE 5: This is a positive way to express that optional fields do not go over HI2. The reason optional fields do not go over HI2 is that some clearly contain content, like the Subject and Comment fields, and the non-optional ones contain sufficient control information to make meaningful IRI. This distinction is easy to specify and does not appear to suffer any loss of functionality.

[E.2.6] The E-mail HI3 shall contain a field that will indicate what application appendix has been used for the encoding of the CC.

NOTE 6: Different levels of information and perhaps even slightly different formats can be expected based on the E-mail application intercepted. These differences are spelled out explicitly in the appendices to the present document. This requirement is to indicate which application appendix to use when interpreting the received CC.

[E.2.7] E-mail HI 3 shall support the ability to send content in the same manner as an IP only content is sent i.e. transfer the constituent IP level packets of the E-mail, including TCP acknowledgements. For the remainder of these requirements this shall be called "IP-packet" delivery.

NOTE 7: For evidentiary reasons, some LEA's may require wire level communications as HI3.

[E.2.8] E-mail HI 3 shall support the ability to send content in the format of the set of commands and data that constitute the E-mail; e.g. the payload of TCP packets in which the E-mail was transported. For the remainder of these requirements this shall be called "application" delivery.

NOTE 8: As described in annex I, this type of HI3 can be derived from intercepting the TCP stream as well as from E-mail application level intercepts. In complex E-mail environments, the HI3 format allows for a hybrid interception approach to produce the same HI3 format throughout.

E.3 General requirements

[E.3.1] The target list (i.e. the list of people who are targets) is typically at least as sensitive as the results of interception and should be protected to appropriate national security standards.

E.4 Requirements mapping

Table E.1: Mapping

Requirement number	Clause number
E.1.1	6.2.1
E.1.2	6.3.1, 6.4.1
E.1.3	6.2.3, 6.3.3, 6.4.3
E.1.4	7.2
E.1.5	6.2.3, 6.3.3, 6.4.3
E.1.6	B.3
E.1.7	6.2.3, 6.3.3, 6.4.3
E.1.8	annex D
E.1.9	annex D
E.1.10	6.2.3, 6.3.3, 6.4.3
E.1.11	6.2.3, 6.3.3, 6.4.3
E.1.12	6.2.3, 6.3.3, 6.4.3
E.2.1	6.2.2, 6.3.2, 6.4.2
E.2.2	6.2.2, 6.3.2, 6.4.2
E.2.3	6.2.3, 6.3.3, 6.4.3 (via abstentia)
E.2.4	6.2.3, 6.3.3, 6.4.3 (via abstentia)
E.2.5	6.2.3, 6.3.3, 6.4.3 (via abstentia)
E.2.6	annex D
E.2.7	annex D
E.2.8	annex D

Annex F (informative): SMTP characteristics

F.1 SMTP service characteristics

The fundamental service characteristic of an SMTP service is that it is a method of pushing E-mail's from one host computer to another. The remaining text below is based on ideas expressed in RFC 2821 [9].

The SMTP service can be divided by participants in two: the SMTP-client and the SMTP-server. Note that the SMTP-server need not be the ultimate destination of any of the E-mail, as is described for an SMTP relay function. Unfortunately RFC 2821 [9] does not provide a concise description of these two participants so one will be provided here.

The SMTP-client is the initiator of all actions while the SMTP-server has the final say as to the validity of these actions. The SMTP-client initiates an SMTP connection, logs onto the server (with no authentication), and proceeds to send as many E-mail messages as the SMTP-client currently has to send to the SMTP-server before quitting the session. The important concept to note is that a single SMTP session can transfer many E-mail messages in it, each message potentially from a different source E-mail address.

The SMTP-server accepts connections and accepts or rejects each action a client attempts to initiate with the server. No SMTP action by the client can be considered valid or complete with out the server accepting the action.

The SMTP service can be divided by functionality into four: SMTP origination; SMTP delivery; SMTP relay; and SMTP gateway. For the purposes of the present document, however, the SMTP gateway service will be viewed as an SMTP delivery service because both services effectively remove the E-mail from SMTP and put it into another form. The enumeration of each of these functionalities can be found in RFC 2821 [9], clause 2.3.8.

Note that in none of the SMTP service functionalities does SMTP deal with the notion of a mailbox. SMTP deals exclusively with the notion of transferring E-mail messages where the domain portion of the SMTP mailbox name is used for routing of the E-mail.

F.2 SMTP protocol characteristics

The SMTP protocol characteristics are enumerated sufficiently in RFC 2821 [9], clauses 3.1 to 3.3. The following characteristics are important to note.

The SMTP login is un-authenticated and often unverified. There is no natural or guaranteed association between the login identity and any of the E-mails sent since multiple E-mails can be sent during a session and each E-mail sent individually specifies the sender with all recipients.

The addresses that accompany the SMTP RCPT TO action are used for routing the E-mail to the destination mailboxes. These addresses, therefore, can be reasonably relied on to be an accurate indicator of the intended recipients of the E-mail.

There is no limit on the number of RCPT TO actions per E-mail message.

The address that accompanies the SMTP MAIL FROM action is used to route replies to the E-mail. This address, therefore, may be spoofed with no loss of sending functionality (i.e. the E-mail can still get to the intended recipient).

There is only one MAIL FROM action per E-mail message.

The addresses specified in the MAIL FROM action and the RCPT TO actions are fully qualified addresses (i.e. mailbox name and domain name).

Annex G (informative): POP3 characteristics

G.1 POP3 service characteristics

The fundamental service characteristic of a POP3 service is that it permits a workstation to dynamically access a mailbox on a server host in a useful fashion. Usually, this means that the POP3 protocol is used to allow a workstation to retrieve mail that the server is holding for it. POP3 is not intended to provide extensive manipulation operations of mail on the server (RFC 1939 [8]).

A normal POP3 service offers gross level queries on the status of the mailbox such as number of messages, size of messages, etc. The main functionality of the POP3 service, as it is used today, is the ability to download E-mail messages and delete E-mail messages from the mailbox.

There is no POP3 service that offers the ability of injecting an E-mail into the Internet or uploading E-mail to the mailbox. In general SMTP or IMAP4 are used for these functionalities.

G.2 POP3 protocol characteristics

The POP3 protocol characteristics are enumerated sufficiently in RFC 1939 [8] clause 3, and in detail in RFC 1939 [8] clauses 4 to 6. The following characteristics are important to note.

The POP3 login name must identify the mailbox to be accessed however there is no standard as to how the mailbox identity is presented. Practically speaking most POP3 logins contain the mailbox name, sans domain name, or the fully qualified E-mail address, however, this is not guaranteed by the protocol.

The senders E-mail address is not interpreted by the POP3 protocol. The senders address is, however, generally contained within the E-mail envelope of a properly formatted RFC 0822 [7] message under the "From" field. Nominally the "From" address is filled in by the MAIL FROM address used in SMTP, however there is no guarantee of this.

All POP3 operations on a mailbox specify messages via integer values, often indicative of the temporal ordering of messages within the mailbox. The only time useful intercept content is provided without a priori knowledge of the state of the mailbox is in response to retrieval commands RETR and TOP.

Annex H (informative): Discussion of webmail interception

H.1 Webmail network topology

A Webmail service is typically offered as part of an ISP service package. It allows for accessing an E-mail service from any Internet enabled computer via a web page, using a plain browser. The added value of a Webmail service is that it does not require specific configuration of an E-mail client and it allows for accessing E-mail from within a network that is connected to the Internet through a very restrictive firewall; most firewalls allow for HTTP traffic.

Although not always appreciated by the original ISP / E-mail provider, a third party can also offer Webmail services based on the E-mail infrastructure of the ISP, by accessing the ISP's POP3 server via the Internet. Therefore, figure H.1 depicts two types of Webmail servers; one within the own ISP's infrastructure and one inside a third party's infrastructure.

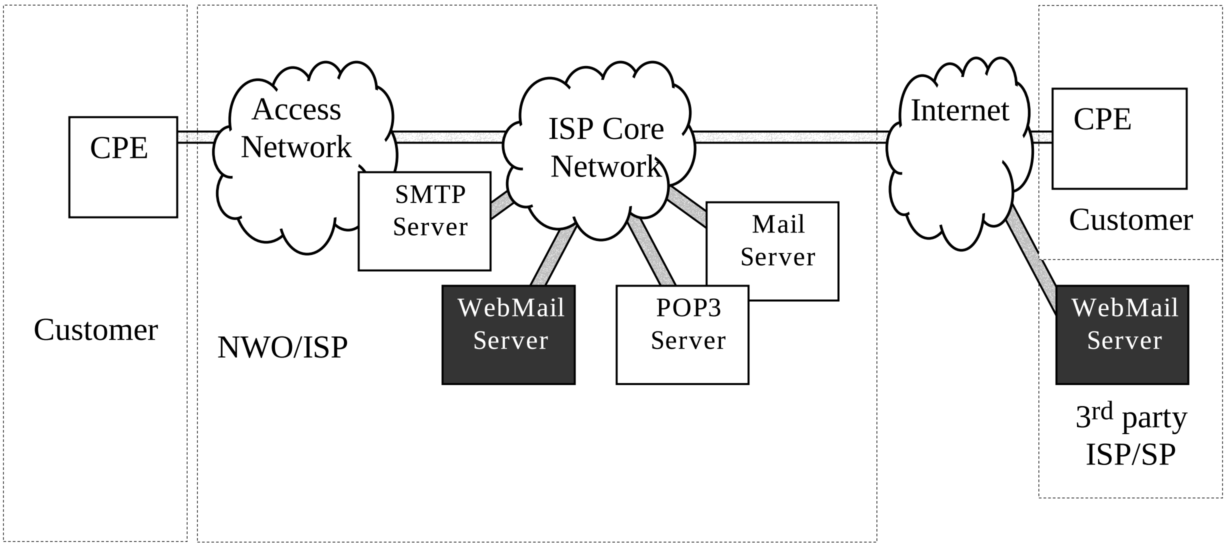

Figure H.1: Webmail network topology

The Webmail service can be used by customers logged-on via one of the ISP's access networks, but is more commonly used directly from the Internet.

H.2 Webmail protocols

As depicted in figure H.2, the Webmail server is positioned as an application server that abstracts the regular E-mail protocols for sending (SMTP) and receiving (POP3) E-mail from the customer by means of a Web application. Typically, the Webmail server accesses the same SMTP and POP3 server(s) in the ISP infrastructure as customers with regular E-mail clients do.

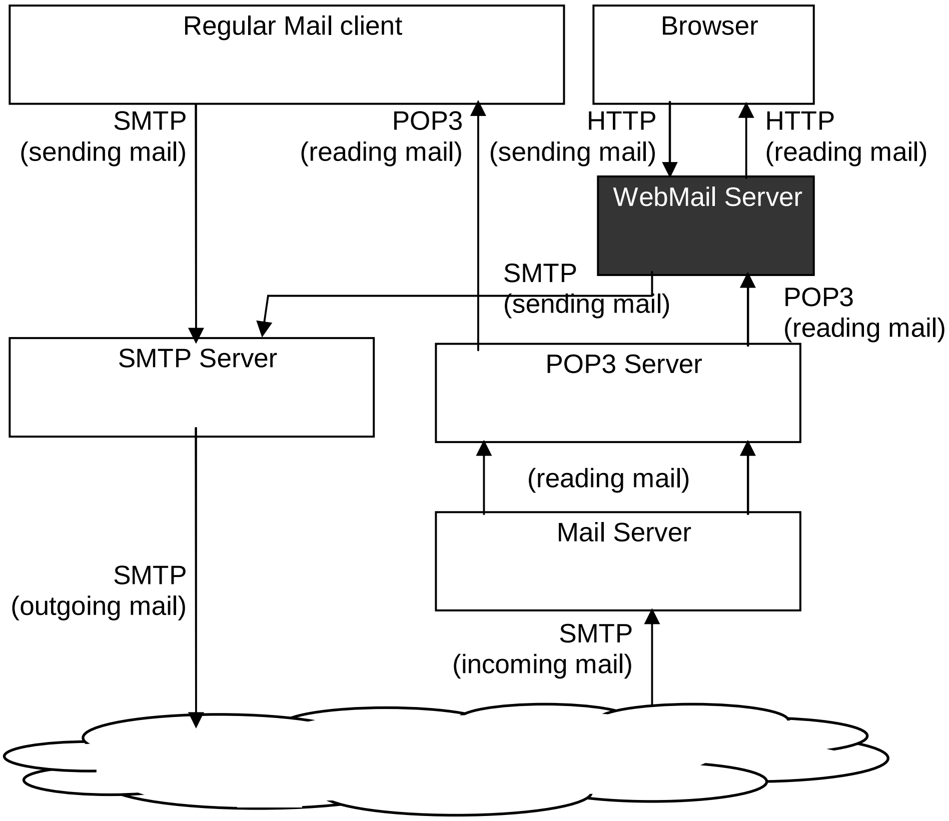

Figure H.2: Webmail protocols

H.3 Webmail interception

The HTTP messages that are exchanged between the Webmail application and the browser are not standardized, i.e. they are fully application dependant, and are therefore subject to potentially many and/or unannounced changes. Additionally, the customer may use a Webmail application from another provider, with obviously yet another implementation and therefore other HTTP messages being exchanged. Therefore, an approach that captures and interprets a HTTP based Webmail protocol will imply implementation and maintainability issues.

Alternative to implementing Webmail protocol interpretation, the SMTP and POP3 interception devices designed regular E-mail interception at the SMTP and POP3 level can be used for intercepting Webmail activity. One issue with this approach is that the IP address from which the customer accesses the Webmail application cannot be easily derived from the captured SMTP/POP3 traffic because this will typically contain the IP address of the Webmail server. Thus, in order to capture the customer's IP address, additional correlation between captured SMTP/POP3 traffic and the HTTP traffic or the web server log files will be required.

In any case, due to the volatility and uncontrolled nature of the Webmail protocols, whatever interception may be possible specifically for Webmail, the expectation should be that E-mail IRI will not be extracted. The advice is to not attempt to define E-mail IRI (or E-mail content) explicitly to accommodate Webmail.

Annex I (informative): Discussion for Driving HI2 of HI3

I.1 Introduction

This clause presents a number of possibilities for intercepting E-mail and shows possible consequences for the HI3 format of the intercepted E-mail message. It is included as in informative annex at this point in time to help generate requirements and focus discussion.

Starting point:

- E-mail messages will be send / received by mail-servers using SMTP over TCP/IP.
- E-mail traffic can be intercepted on various layers in the E-mail transmission protocol.
- In order to intercept an E-mail, the Mail address(es) in the E-mail require inspection.
- In order to check the Mail address(es), processing of the intercepted data may be required.

I.2 Discussion

I.2.1 Introduction

Figure I.1 shows an example protocol stack for transmitting E-mail messages.

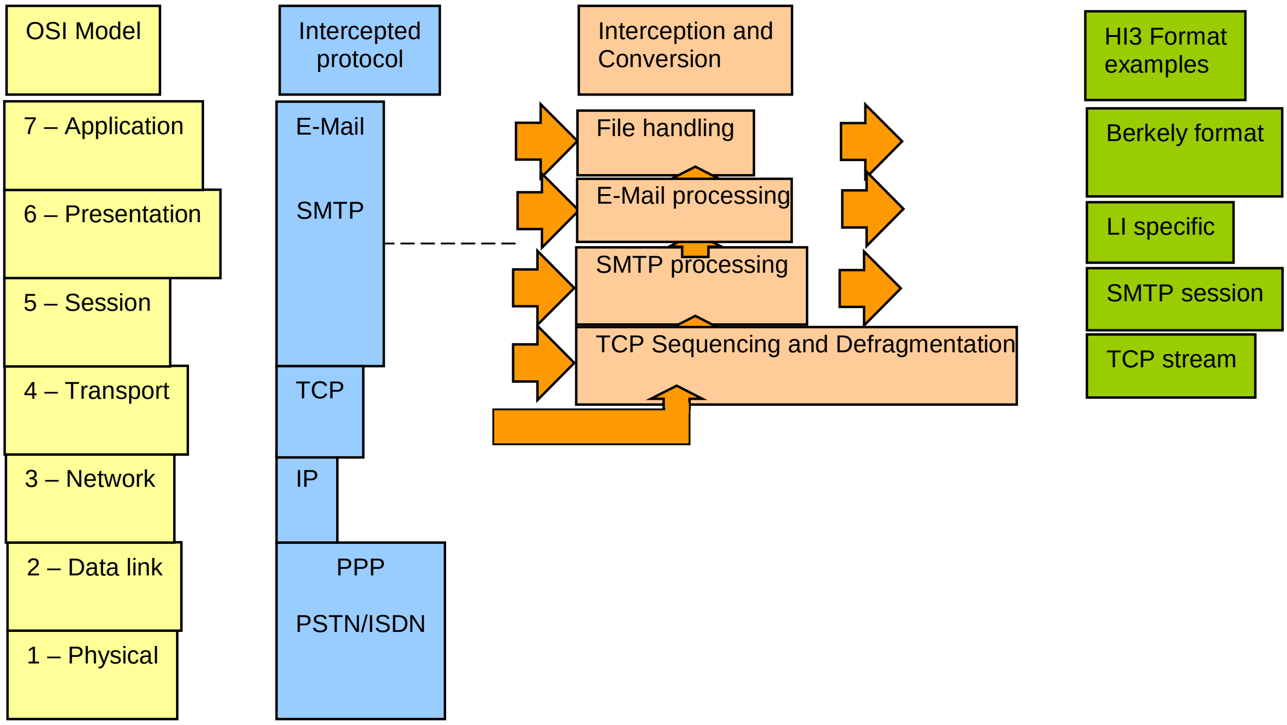

Figure I.1: Discussion diagram

In the following clauses, interception on each of the protocol layers is discussed.

I.2.2 IP packets

Data source: Layer 3 network filter

HI3 Output: N/A

An E-mail message cannot be intercepted by just copying the stream of IP datagrams that may contain E-mail. The problem here is the identification of the right E-mail message, that is, to inspect the message for the target's E-mail address (or even detecting the presence of SMTP traffic in the IP datagrams). Therefore, IP datagrams are only useful as input to further processing, i.e. TCP Sequencing and Reassembly.

I.2.3 TCP packets

Data source: Layer 3/4 network filter

HI3 Output: TCP packets

E-mail messages can be intercepted by inspecting the TCP stream from or to the E-mail server (inspect all port 25 traffic for a given IP address). However, in order to reliably inspect the TCP payload for the occurrence of the target's E-mail address and in order to allow for reconstruction of the E-mail payload in case of a hit, the TCP packets must be re-sequenced and possible defragmented. If the raw TCP packets were to be inspected as they came in, the occurrence of "out-of-sequence" packets or fragmented TCP packets could prohibit successful identification of the targets E-mail address. Additionally, some interpretation of the SMTP encoding must be performed, in order to not accidentally intercept an E-mail that contains, for example, the target's E-mail address as part of the content. This approach allows delivery of all TCP frames the make up the SMTP session that transmitted the E-mail message. A downside of this approach is that the extraction of HI2 information in relation to the intercepted E-mail is not straightforward.

I.2.4 SMTP packets

Data source: TCP sequencing and defragmentation process; or

Copy forward from E-mail server (SMTP)

HI3 Output: ASCII or raw TCP representation of the SMTP session

More reliable detection of the target's E-mail address and more straightforward extraction of HI2 information can be achieved by processing the SMTP session itself. This requires implementation of an SMTP state machine, similar to that of the receiving end of an E-mail server, but less sophisticated. Data is either received from a TCP sequencing and reassembly process or by means of a CopyForward from an E-mail server (note). In this approach, all attributes of the E-mail message are available and the HI3 can consist of either an ASCII representation of the SMTP session or of the TCP packets that contain the SMTP session.

NOTE: In latter case, it is also possible to implement interception functionality in the E-mail server itself, so that it can identify a target's E-mail messages and only forward those messages that require interception to the interception platform. The downside of the approach is the need for target information in an operational platform and the possibility of accidental disclosure of the interception (for example due to delivery failure notification in case the interception platform is down).

I.2.5 E-mail messages

Data source: SMTP reassembly process; or

Proprietary interface on the E-mail server

Output: Specific representation of the E-mail message

If the LEA does not allow for sending the data of the SMTP session as HI3 for an intercepted E-mail, further processing of the SMTP data into some specific representation of the E-mail message is required. This format can be LI specific or standardized, e.g. the Berkely format. The latter format could also be copied directly from the E-mail server.

I.3 Conclusion

The approach used for intercepting E-mail has a lot of impact on the HI3 format. Therefore, the various approaches to intercepting E-mail must be discussed, before one or more HI3 formats can be selected.

History

Document history		
V1.1.1	February 2004	Publication