ETSI TS 102 232-2 V3.6.1 (2013-10)

Technical Specification

Lawful Interception (LI);
Handover Interface and
Service-Specific Details (SSD) for IP delivery;
Part 2: Service-specific details for messaging services

Reference

RTS/LI-00108-2

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, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

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://ipr.etsi.org).

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).

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [3].

The ASN.1 module is also available as an electronic attachment to the original document from the ETSI site (see details in annex D).

Introduction

The present document describes what information is required for the handover of intercepted IP-based messaging traffic from a Communications Service Provider 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 102 232-1 [3].

The Recommendation ITU-T 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 the entire 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 a messaging service interaction.

The present document is intended to be general enough to be used in a variety of messaging 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 messaging 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 asynchronous messages. The present document also contains a stage 2 like description of when Intercept Related Information (IRI) and Content of Communication (CC) need to be sent, and what information it needs to 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 102 232-1 [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 3GPP TS 33.108 [5], TS 101 671 [4], TS 101 331 [1] and TR 101 944 [i.1].

2   References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1   Normative references

The following referenced documents are necessary for the application of the present document.

[1]   ETSI TS 101 331: "Lawful Interception (LI); Requirements of Law Enforcement Agencies".

[2]   Void.

[3]   ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".

[4]   ETSI TS 101 671: "Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic".

NOTE: Periodically TS 101 671 is published as ES 201 671. A reference to the latest version of the TS as above reflects the latest stable content from ETSI/TC LI.

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

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

[7]   IETF RFC 5322: "Internet Message Format".

NOTE 1: IETF RFC 5322 obsoletes IETF RFC 2822: "Internet Message Format".

NOTE 2: IETF RFC 2822 obsoletes IETF RFC 0822: "Standard for the format of ARPA Internet text messages".

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

[9]   IETF RFC 5321: "Simple Mail Transfer Protocol".

NOTE: IETF RFC 5321 obsoletes IETF RFC 2821: "Simple Mail Transfer Protocol".

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

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

[12]   ISO 3166-1: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".

[13]   IETF RFC 4954: "SMTP Service Extension for Authentication".

NOTE: IETF RFC 4954 obsoletes IETF RFC 2554: "SMTP Service Extension for Authentication".

[14]   Void.

[15]   IETF RFC 3493: "Basic Socket Interface Extensions for IPv6".

[16]   IETF RFC 4422: "Simple Authentication and Security Layer (SASL)".

NOTE: IETF RFC 4422 obsoletes IETF RFC 2222: "Simple Authentication and Security Layer (SASL)".

[17]   IETF RFC 3207: "SMTP Service Extension for Secure SMTP over Transport Layer Security".

[18]   IETF RFC 2595: "Using TLS with IMAP, POP3 and ACAP".

[19]   IETF RFC 4616: "The PLAIN Simple Authentication and Security Layer (SASL) Mechanism".

[20]   IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".

[21]   IETF RFC 2046: "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

[22]   Void.

[23]   ETSI EN 300 356 (all parts): "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface".

[24]   IETF RFC 3066: "Tags for the Identification of Languages".

[25]   Recommendation ITU-T E.164: "The international public telecommunication numbering plan".

[26]   IETF RFC 3696: "Application Techniques for Checking and Transformation of Names".

[27]   Recommendation ITU-T E.212: "The international identification plan for public networks and subscriptions".

[28]   Void.

[29]   IETF RFC 2806: "URLs for Telephone Calls".

[30]   ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".

[31]   IETF RFC 791: "Internet Protocol".

[32]   IETF RFC 3261: "SIP: Session Initiation Protocol".

[33]   IETF RFC 4282: "The Network Access Identifier".

[34]   IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[35]   IETF RFC 6335: "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry".

[36]   ETSI TS 129 002: "Digital cellular telecommunications system (Phase 2+); Universal Mobile
            Telecommunications System (UMTS); Mobile Application Part (MAP) specification
            (3GPP TS 29.002)".

[37]   ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+); Universal Mobile
            Telecommunications System (UMTS); Numbering, addressing and identification
            (3GPP TS 23.003)".

[38]   ETSI TS 102 232-5: "Lawful Interception (LI); Handover Interface and Service-Specific Details
            (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services".

2.2   Informative references

The following referenced documents are not necessary for the application of the present document but they assist the
user with regard to a particular subject area.

[i.1]   ETSI TR 101 944: "Telecommunications security; Lawful Interception (LI); Issues on IP
            Interception".

[i.2]   ETSI TR 102 503: "Lawful Interception (LI); ASN.1 Object Identifiers in Lawful Interception and
            Retained data handling Specifications".

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 5322 [7], clause 6.

IMAP4: protocol used to manipulate mailbox parameters on a server

   NOTE: As 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: As 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: As described in RFC 5321 [9].

3.2   Abbreviations

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

AAA   Authentication, Authorization, and Accounting
APOP   POP3 authentication message
ASCII   American Standard Code for Information Interchange
ASN.1   Abstract Syntax Notation One
BER   Basic Encoding Rules
CC   Content of Communication
CIN   Communication Identity Number
CPE   Customer Premises Equipment
CR   Change Request
CSP   Communication Service Provider
HI2   Handover Interface port 2 (for Intercept Related Information)
HI3   Handover Interface port 3 (for Content of Communication)
HTTP   Hyper Text Transfer Protocol
IMAP   Internet Message Access 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
LIID   Lawful Interception IDentifier
MF   Mediation Function
MMS   Multi Media Messaging Service
MTA   Mail Transfer Agents
NAPT   Network Address and Port Translation
OID   Object IDentifier
PIN   Personal Identification Number
POP3   Post Office Protocol version 3
PPP   Point to Point Protocol
PSTN   Public Switched Telecommunication Network
RCF   Request For Comments
RETR   POP3 RETRieve message
RTP   Real Time Protocol
SASL   Simple Authentication and Security Layer
SMS   Shot Message Service
SMTP   Simple Mail Transfer Protocol
SP   Service Provider
TC   Technical Committee
TCP   Transmission Control Protocol
TLS   Transport Layer Security
UID   Unique Identifier
UM   Unified Messaging
UMS   Unified Messaging System

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 5322 [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 Law Enforcement Agencies (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 set-up the E-mail communication and to terminate the E-mail communication and are outside of the traditional RFC 5322 [7] formatted E-mail. This allows for different interception solutions without burdening the Mediation Function (MF) with the responsibility of "cleaning" up said differences in input.

4.2 Unified messaging

Unified Messaging (**UM**) is the integration of different electronic messaging and communications media (e-mail, SMS, Fax, voicemail, video messaging, etc.) technologies into a single interface, accessible from a variety of different devices. A "voicemail only" system without capability for fax, video, etc. is still regarded as an UM system in the present document.

For the purpose of lawful interception, a target's UM service might be intercepted as part of a "network intercept". This is for example the case when the target accesses his UM box from his own mobile terminal. In that case handover is covered by [5]. However if the target accesses his mailbox from a public terminal (using a PIN code), the access event is in scope of the present document. The same applies for additional UM services that might be offered by a CSP, such as e-mail notifications, SMS notifications, the ability to change a greeting message or PIN using a web interface.

While e-mail services can be considered part of UM, for handover of intercepted e-mail a CSP shall use the EmailCC and EmailIRI structures.

5 E-mail 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 or 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.
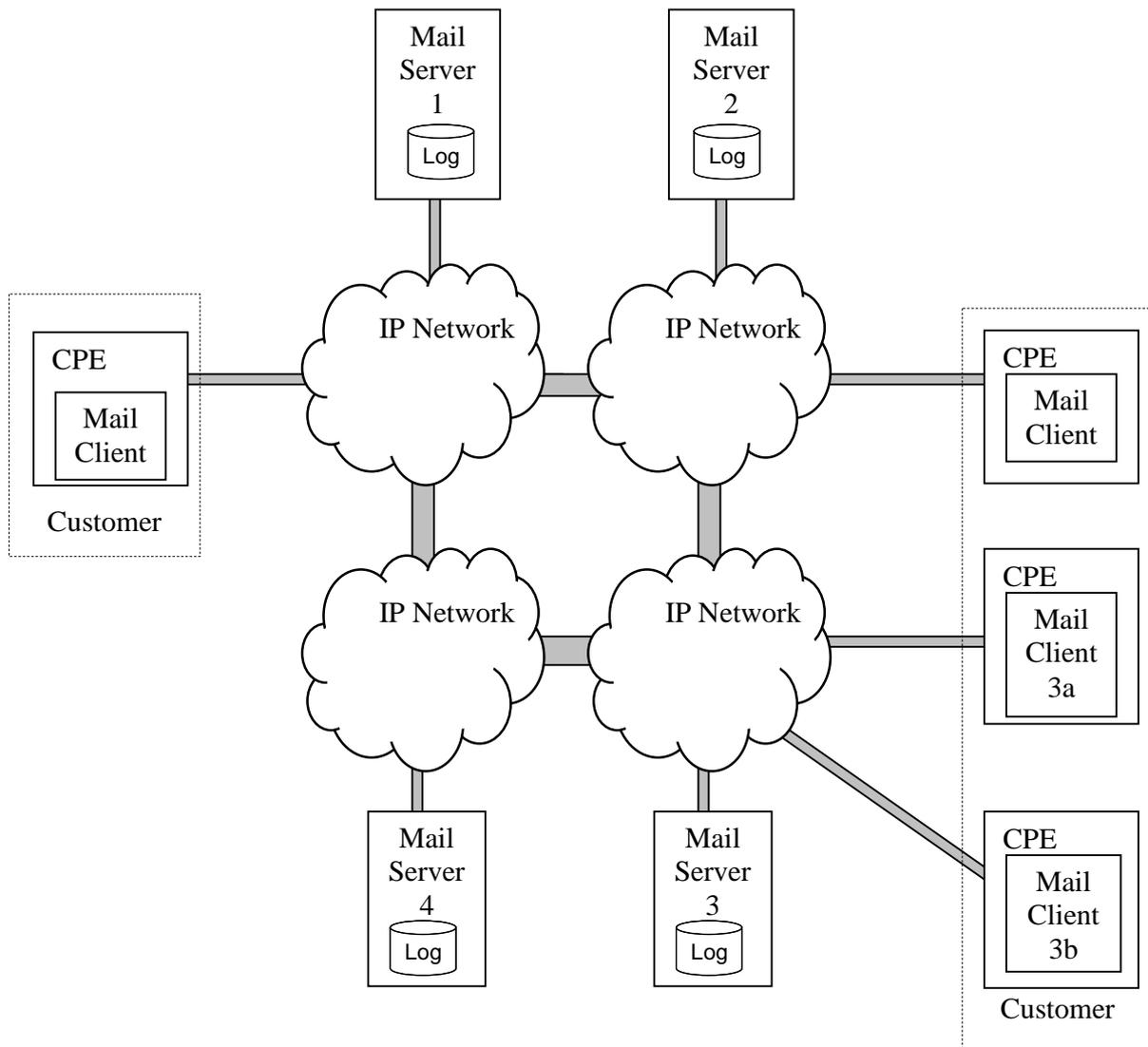
Figure 1: Reference network topology

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.
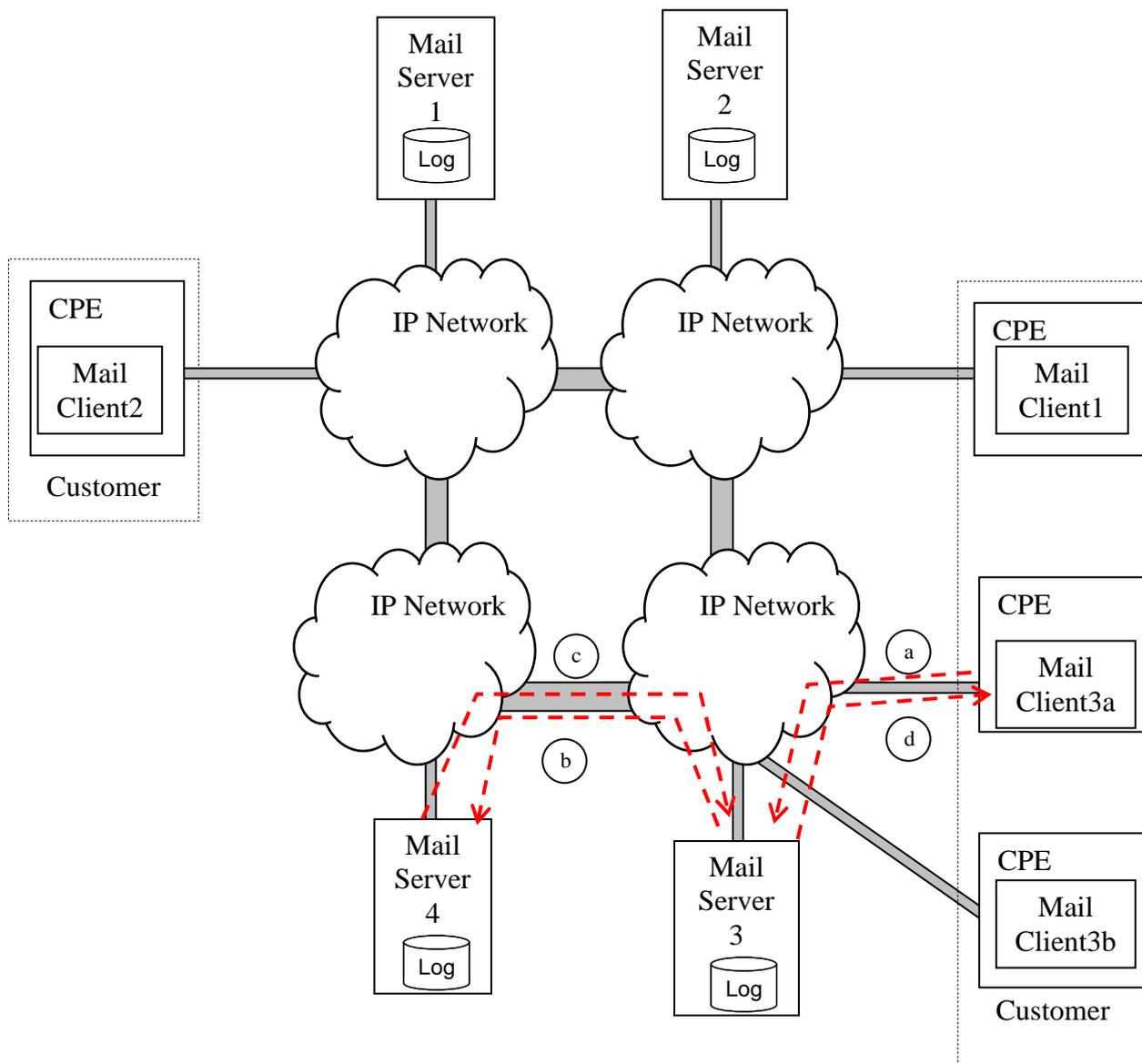
Figure 2: E-mail send failure

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.
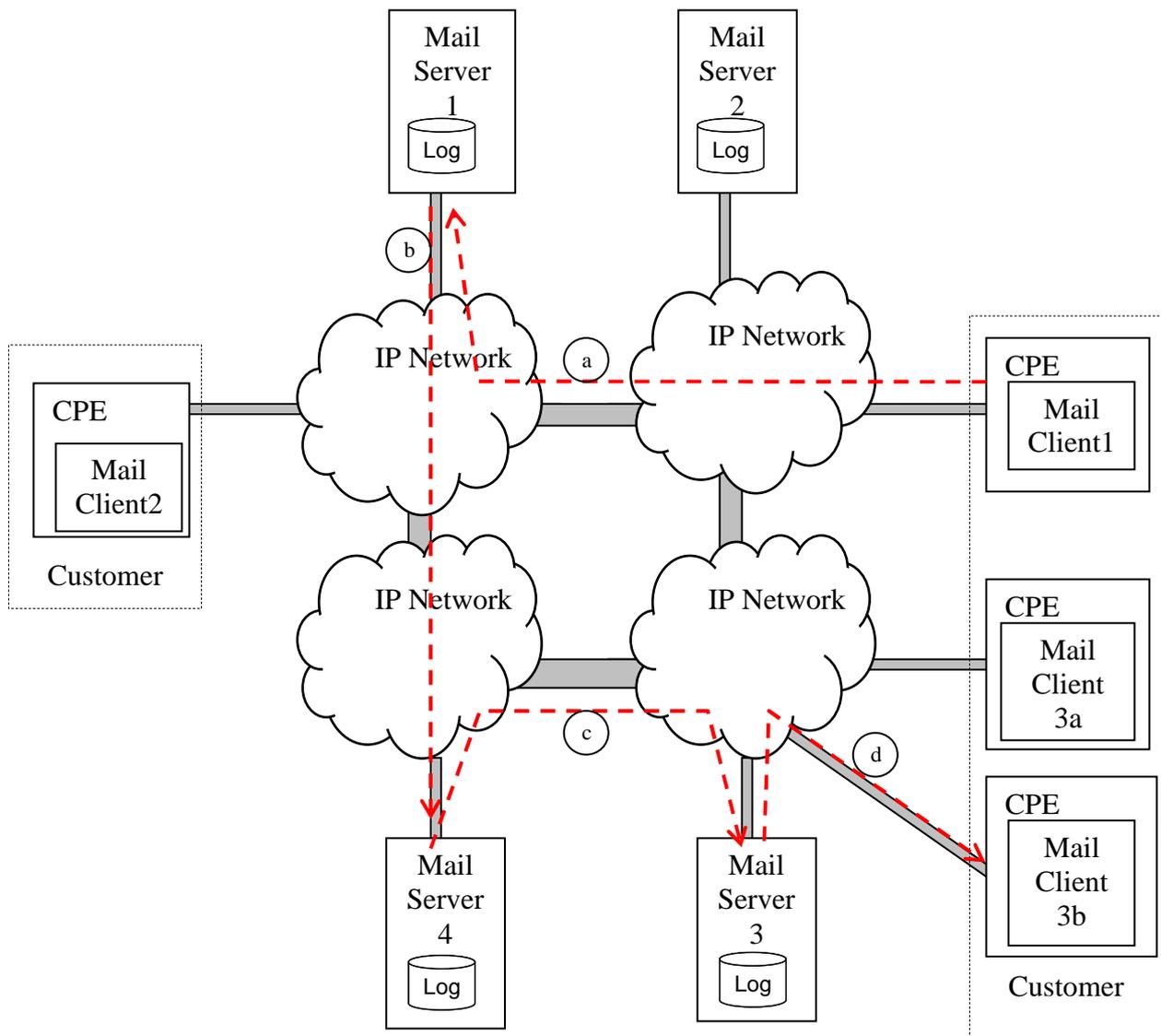
Figure 3: E-mail send success

5.2.3   E-mail download detail

This scenario enumerates the processes that shall 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 they 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.
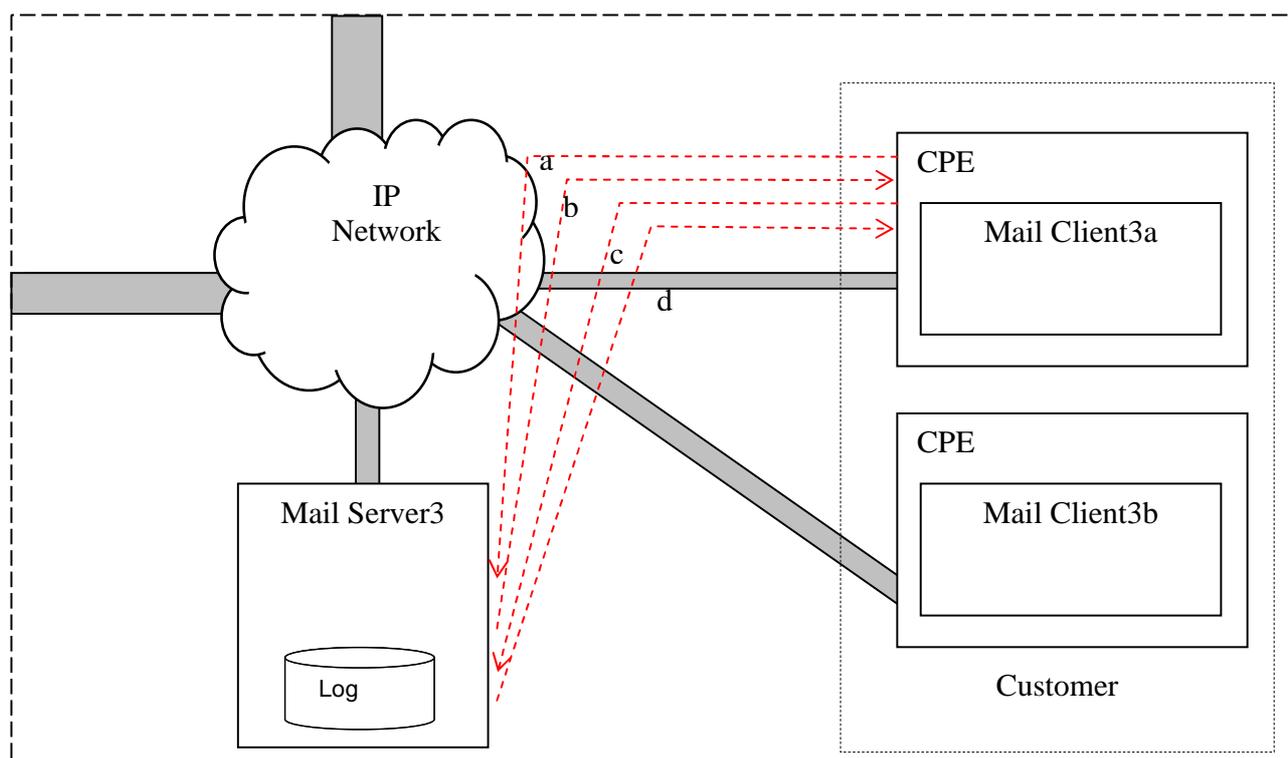
Figure 4: E-mail download detail

5.2.4   E-mail send detail

This scenario enumerates the processes that shall 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.
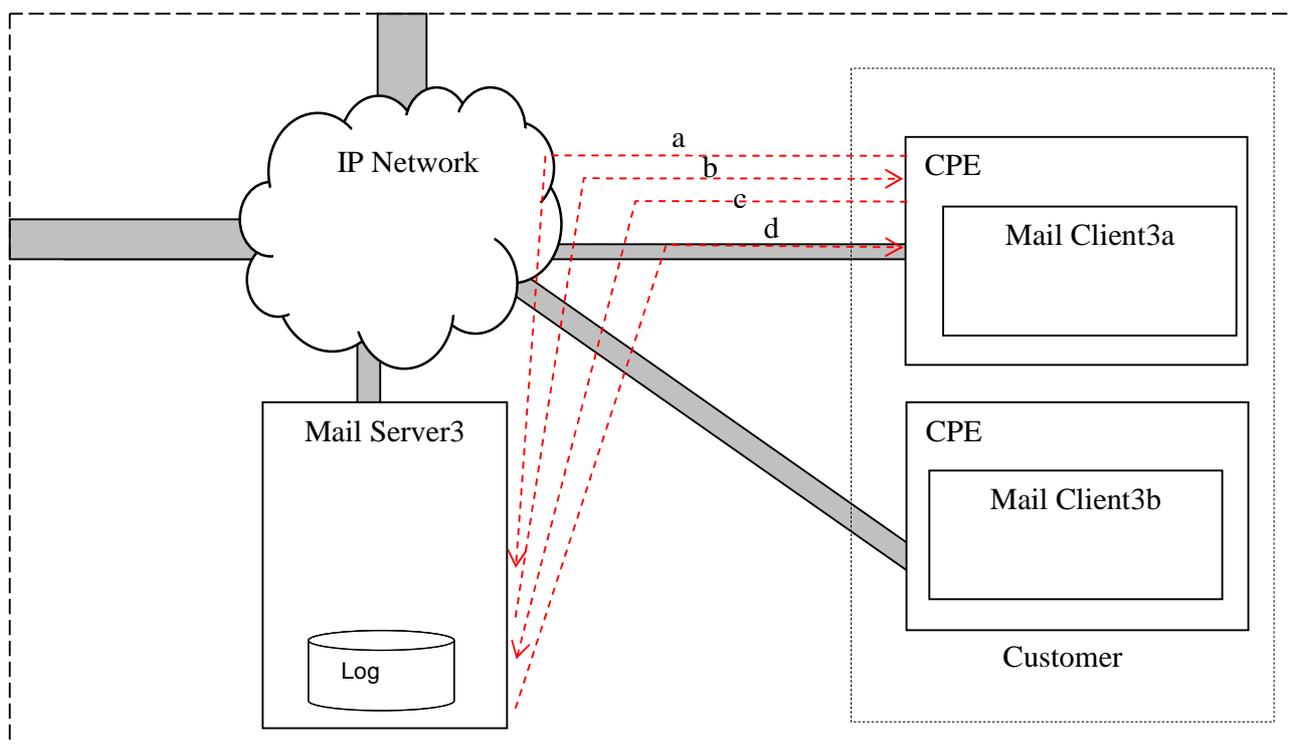
Figure 5: E-mail send detail

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 shall 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 5322 [7] E-mail envelope and text or, at the other extreme, the captured content may be the whole E-mail session. What shall be present is the RFC 5322 [7] E-mail envelope and text for E-mails sent by the target.

This clause fulfils requirements [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]	TS 101 671 [4], IP address
Client IP	[E.1.7]	TS 101 671 [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
AAAInformation	[E.1.13]	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 cannot 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 cannot 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 set-up 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.

In case authenticated SMTP, as defined in RFC 4954 [13], is used, the AAAInformation contains the username, the authentication method, the challenge and response string and the result. As defined in requirements [E.1.13] and [E.2.3], this information shall be available in the case of application layer interception. In the case of IP packet interception, it shall be sent as part of HI3 in IP packet format, in which case there is no explicit mapping onto an ASN.1 structure.

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 shall 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 5322 [7] E-mail envelope and text, or, at the other extreme, the captured content may be the whole E-mail session. What shall be present is the RFC 5322 [7] E-mail envelope and text for E-mails received by the target.

This clause fulfils requirements [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]	TS 101 671 [4], IP address
Client IP	[E.1.7]	TS 101 671 [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 set-up 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 shall be considered a separate E-mail Download Event. In the case where not the full E-mail content is downloaded by the user, but just the header and some lines at the top of the E-mail, this shall be signalled by using the "E-mail partial download" event instead of the regular "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 5322 [7] E-mail envelope and text, or, at the other extreme, the captured content may be the whole E-mail session. In the case of an E-mail partial download, the captured content will contain the part of the E-mail that was downloaded by the user. What shall be present is the RFC 5322 [7] E-mail envelope and text for E-mails received by the target.

This clause fulfils requirements [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]	TS 101 671 [4], IP address
Client IP	[E.1.7]	TS 101 671 [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
AAAInformation	[E.1.13]	Clause 7

In case POP3, as defined in RFC 3493 [15], or IMAP4 with a clear-text username and password as defined in RFC 3501 [10], is used, the AAAInformation contains the username, the password and the result. As defined in requirements [E.1.13] and [E.2.3], this information shall be available in the case of application layer interception. In the case of IP packet interception, it shall be sent as part of HI3 in IP packet format, in which case there is no explicit mapping onto an ASN.1 structure.

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;

- IMAP.

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 IDs 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 Partial Download	Partial 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 server 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.

7.10   AAAInformation

This structure contains the various attributes related to authentication in either the POP3, IMAP4 or SMTP protocol. Whether the values may be present is depending on national legislation.

8   Unified Messaging events

UM events that happen after invocation of the intercept shall be signalled using the MessagingCC and MessagingIRI ASN.1. If the Messaging events are created/formatted for LEA delivery by an LI mediation system, the original-message element in the MessagingIRI may, up to agreement between CSP and LEA, contain the "raw" IRI event as generated by the UM system. The event generated by the UM system shall be translated onto an event defined in the MessagingIRI. If no translation is possible, the LEA can use the raw event for analysis. The box-identifier can be used to uniquely identify a message box in the case where multiple boxes are under intercept within the same LIID. The system-identifier element identifies the specific system that generated the event. The exchange of information regarding the systems and raw event documentation is up to bilateral agreement between CSP and LEA and is outside the scope of the present document.

The status of the current operation can be signalled using the Messaging-Status:

- unknown:
  it is unknown what the status is (e.g. a raw event was formatted and the mediation function was unable to interpret its status);

- not-applicable:
  a status is not applicable for the event because it is implicit (e.g. a login event, mailbox lock);

- operation-failed:
  the operation failed (for example a refused login);

- operation-succeeded:
  the operation succeeded (for example a voicemail message was successfully deleted);

- operation-cancelled:
  the user cancelled the operation in progress (for example a target only listens to part of a voicemail message);

- operation-started:
  the operation was started but its outcome is still unknown (for example a message deposit was started);

- operation-lost:
  the operation was started but its outcome was lost (for example: the mediator lost track of the operation).

8.1 Delivery of CC

A number of UM events shall trigger delivery of CC. This can for example be the UM message deposited or the greeting message that was deposited or changed. Table 5 indicates which events shall trigger CC.

Table 5: Unified Messaging events that shall trigger CC delivery

Structure	Element (event)
Messaging-Event	deposit
Messaging-Event	retrieve
Messaging-Event	delete
Messaging-Event	save
Messaging-Box-Event	greeting-record
Messaging-Box-Event	greeting-change
Messaging-Box-Event	greeting-delete
Messaging-Box-Event	greeting-enable
Messaging-Box-Event	greeting-disable
Messaging-Box-Event	greeting-play
Messaging-Notification-Event	sms
Messaging-Notification-Event	sms-deposit
Messaging-Notification-Event	sms-slamdown
Messaging-Notification-Event	sms-pin-reminder
Messaging-Notification-Event	email
Messaging-Notification-Event	fax-to-email

A CIN shall be created for each logical sequence of UM events. An example of a logical sequence is a target that logs in to the UM box until he logs out. All intermediate events (e.g. message retrieve, message delete, greeting change) shall have the same CIN. When both IRI and CC is sent, the event-identifier element shall be used to uniquely identify the event within the same CIN. This helps the LEA to correlate the events (a target could for example retrieve three messages in the same session). If one event delivers multiple parts of CC (e.g. text and graphics) the content-identifier can be used to identify the unique content streams within the same event-identifier.

Depending on the type of CC content, either the MessagingCC or MessagingMMCC payloads may be used. The MessagingMMCC payload may be used when the signalling capabilities from TS 102 232-5 [38] are required. Otherwise, the MessagingCC payload may be used.

The sequence-number parameter may be used to chunk the MessagingCC in smaller pieces of content, in a scenario where the CC is streamed and buffering is not desirable. Numbering shall start at 0. The last piece of MessagingCC shall in that case be signalled with the end-of-sequence parameter. If sequence-numbering is not used, the content parameter shall contain all data. The type of content in the MessagingCC is signalled using the content-type element which shall contain the mime-type as defined in RFC 2045 [20] and RFC 2046 [21]. A common use case is the delivery of a set of RTP streams that contains the call legs between the user and the UM-system. The RTP streams start once a user connects to the UM-system. Therefore, the RTP legs should be correlated to the HI2 'connect' event. The table 6 describes the MessagingCC signalling required for the separate CC RTP streams. Alternatively, when detailed signalling information is available, the MessagingCC payload may be used.

Table 6: CC signalling for streaming RTP within a UM environment

Structure	Value
CCPayload.payloadDirection	fromTarget/toTarget
MessagingCC.event-identifier	MessagingIRI.event-identifer of 'connect' event
MessagingCC.content-identifier	'0' for 'fromTarget' direction/'1' for 'toTarget' direction
MessagingCC.content-type	mime-type translated from RTP Payload Type
MessagingCC.content	Extracted RTP Payload according to mime-type

The content of an SMS message delivered by the UM-system shall be signalled as MessagingCC with a content-type of 'text/plain' and an optional character encoding.

NOTE 1: It is possible that one UM event can result in multiple IRI/CC deliveries, for example if the target receives an SMS and e-mail notification at the same time.

NOTE 2: If a target's mobile terminal and UM box are both intercepted, it is very likely that duplicate delivery will take place when the target accesses his own message box. As the intercepted material originates from different systems, the CSP may not be able to correlate these different streams. As a countermeasure, up to agreement between CSP and LEA, it may be decided not to deliver CC from the UM system when the target accesses his own message box.

8.2 Messaging events

The Messaging-Event structure is used to indicate that a message is manipulated within the UM system. The following events can be signalled:

- deposit:
  a message is delivered to the target's UM box;

- retrieve:
  a message is retrieved by the target;

- delete:
  a message is deleted by the target;

- save:
  a message is saved by the target;

- slamdown:
  deposit of a message is aborted (caller "slams down" before speaking);

- greeting-play:
  a greeting is played for a party;

- language-change:
  the target changes his language preference;

- pin-security-enable:
  the target enables PIN security. Without PIN security, access to a messaging system may be granted by only verifying the end-user device. With PIN security, the PIN authentication is enforced in every access attempt towards the messaging system;

- pin-security-disable:
  the target disables PIN security.

8.3 Messaging box events

The Messaging-Box-Event structure is used to signal operations on the target's message box. The following events can be signalled:

- login:
  the target logs in to the box;

- logout:
  the target logs out from the box;

- lock:
  the target locks the box;

- unlock:
  the target unlocks the box;

- activate:
  a box is activated (for example: the target activates the voicemail service);

- deactivate:
  a box is deactivated;

- delete:
  a box is deleted;

- pin-change:
  the target changes the pin-code of the box;

- greeting-record:
  the target records a new greeting message;

- greeting-change:
  the target changes an existing greeting message;

- greeting-delete:
  the target deletes a greeting message;

- greeting-enable:
  the target enables a greeting message;

- greeting-disable:
  the target disables a greeting message;

- notification-enable:
  the target enables notification in case of new messages;

- notification-disable:
  the target disables notification in case of new messages;

- disconnect:
  the target is disconnected from the box without performing a logout;

- connect:
  a party (either the target or the third party) connects to the messaging system and has not yet performed further operations.

8.4 Messaging notification events

The Messaging-Notification-Event structure is used to signal the LEA that a notification was sent to the target. The following messages can be signalled:

- sms:
  an SMS message was sent to the target;

- sms-deposit:
  the target is notified that a new message is available in the box;

- sms-slamdown:
  the target is notified that a user disconnected before delivering a message to the UM system (for example: user disconnects during a voicemail greeting before the "beep");

- sms-pin-reminder:
  a reminder message with the PIN of the message box was sent to the target;

- email:
  an e-mail message was sent to the target;

- fax-to-email:
  the UM system received a fax message and forwarded it as an e-mail to the target;

- mms:
  an MMS message was sent to the target.

8.5   Messaging call events

The Messaging-Call-Event is used to signal call events related to the messaging system. One event "callout" is currently supported to signal the LEA that the target instructed the UM system to set up a call with the sender of a messaging event.

8.6   Signalling of party information

The generic information to signal the party information related to the messaging event is in the Messaging-Party-Information structure. The party-qualifier signals if the party was originating, terminating, associated or if it was unknown. The party-identities are described in table 7. The optional party-validity signals whether the CSP has assured the party identity. The optional copy-qualifier signals whether the party identity was directly addressed, carbon copied or blind carbon copied.

> NOTE 1: The associated party qualifier can be used to signal the association between a party and a specific element within the messaging system. A common use case is a user configuring a specific greeting for a limited selection of parties.

> NOTE 2: To avoid confusion: the party-validity does not imply that the CSP identified an actual person.

Table 7: Parameters and references of party-identity

Party identity	Parameters	Comments or references
Telephone number	msisdn, e164-format, tel-url, fax-url, modem-url sip-uri, sips-uri	msisdn, and e164-format, are defined in the Recommendation ITU-T E.164 [25]. tel-url, fax-url, and modem-url are defined in the RFC 2806 [29]. These identities may not be available in the UMS. sip-uri and sips-uri are defined in the RFC 3261 [32]. These identities may not be available in the UMS.
Email-address	email-address	RFC 5322 [7], RFC 5321 [9] and RFC 3696 [26] of IETF define the email-address.
IP address	ip-address or ip-address-and-port	It is recommended to get both source IP address and source port, if available. IP address may be insufficient if the party is using a NAPT based Internet access. ip-address-and-port is made of port-number and of ip-address. They are defined in the RFC 6335 [35] of IETF, and in RFC 791 [31] for IP V4 and RFC 2460 [34] for IP V6. The important elements are those related to the client The elements regarding to the server are useful if the UMS is complex, or based on interconnected heterogeneous UMS servers, which let exchange of voice or multimedia messages between different boxes and different operators, through some NAPT. It will be useful to determine if it is a client or server side by using the parameter "party-information", and related parameter "Messaging-Party-Qualifier". It will be easy to determine if the party is originating or is the destination.
Mobile identity	imsi, imei or nai	imsi is defined in 3GPP TS 23.003 [37] ,clause 2.2. For International Mobile Subscriber Identity, Recommendation ITU-T E.212 [27]. imei is defined in 3GPP TS 23.003 [37], clause 6. This identity may not be available in the UMS. nai is the network access identity. It is defined in 3GPP TS 33.108 [5], and based on the RFC 4282 [33]. This identity may not be available in the UMS.
Alphanumeric parameter	alphanumeric	The usage of the alphanumeric parameter is described in TS 101 671 [4], clause A.3.3.

The Messaging-Trigger is used to signal the source of the event:

- unknown:
  it is not known where the event originated;

- user:
  user action, either target or someone who is depositing a message. If the difference between user and user-agent is unclear, user should be preferred;

- user-agent:
  web-application or mobile-application acting on behalf of the user;

- system:
  i.e. an automated process cleaning a user's mailbox after inactivity;

- system-operator:
  manual intervention by CSP personnel.

8.7 Messaging properties

The Messaging-Property structure is used to signal additional information about a certain Messaging event. The following properties can be signalled:

- pincode:
  the PIN code used in events where a PIN code is applicable;

- priority:
  the priority of a message.
  Note that messaging systems often use other priorities. The most commonly used priorities have been implemented in the present document:

  - low;

  - medium;

  - high;

  - private.

- greeting-type:
  the type of greeting:

  - general;

  - name:
    greeting where the user only specifies his/her name;

  - personal:
    greeting recorded by the user;

  - absence:
    greeting specifically indicating the absence of a user. Some messaging systems might only play an absence greeting and do not allow further message deposits;

  - number:
    greeting where the messaging system reads the number of the box.

- notification-type:

  - empty-call:
    used for sending a notification when a user connected to a box but did not leave a message after the 'beep';

  - lost-call:
    used for sending a notification when a user called another user that did not answer the call;

  - message-to-email:
    used for sending an e-mail notification to the user when the user's box receives a message;

  - read-report:
    used for sending a read report notification when it was requested by the originating party;

  - delivery-report:
    used for sending a delivery report notification when it was requested by the originating party;

- allow-delivery-report:
  used for sending a notification to the messaging system that indicates it is allowed to send a delivery-report to the originating party;

- deny-delivery-report:
  used for sending a notification to the messaging system that indicates it is not allowed to send a delivery-report to the originating party.

- language:
  the language preference within the messaging system;

- message-identifier:
  identifier that identifies a message within the messaging system;

- subject:
  the subject of a message;

- user-agent:
  a string identifying the application that was used to trigger the event (a browser for instance);

- password:
  a password used in events where a password is applicable;

- message-status:

  - indeterminate:
    the message status cannot be determined;

  - expired:
    the message expired;

  - retrieved:
    the message was retrieved;

  - rejected:
    the message was rejected;

  - deferred:
    the message was deferred;

  - forwarded:
    the message was forwarded;

  - unrecognized:
    the message was not recognized by the terminating party;

  - unreachable:
    the message did not reach the terminating party;

  - read:
    the message was read;

  - deleted-without-being-read:
    the message was deleted without being read;

  - delivery-condition-not-met:
    the delivery condition was not met by the terminating party.

- requested-reports:

    - delivery:
      a delivery report was requested by the originating party;

    - read:
      a read report was requested by the originating party;

    - delivery-and-read:
      both read and delivery reports were requested by the originating party.

- expires:
  expiry date related to the event (for example: the messaging system may delete an undeliverable message once the expiry date has passed);

- message-date:
  the date of the message.

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 5321 [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 5321 [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 5321 [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 5321 [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

Field name	Contents
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 or the Resent-Message-ID as specified in the RFC 5322 [7] E-mail header attribute "Message-ID" or "Resent-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.2.3 E-mail partial download event

A POP3 partial download event should be generated after the POP3 client has sent TOP command and the server has responded the partial 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

Field name	Contents
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 5322 [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 or the Resent-Message-ID as specified in the RFC 5322 [7] E-mail header attribute "Message-ID" or "Resent-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 attempt	Client	Report
POP3 log on failure	Client	Report
POP3 log on	Client	Begin
E-mail download	Client	Continue/Report
E mail partial 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

B.5 POP3 HI3 delivery of Content of Communication

Content of Communication (CC) shall contain the complete data of all POP3 sessions initiated by a target. Sessions extend from the AUTHORIZATION state commands until the UPDATE state commands. USER, PASS, APOP and QUIT have to be included.

POP3 provides the possibility to extend individual sessions to reasonable periods of time (the RFC states that an auto logoff timer shall be a minimum of 10 minutes and a client may keep the session alive by sending periodic NOOP commands), making it impractical to deliver CC only after the session is closed. To keep the delay between original communication and delivery of CC to an amount acceptable to LEAs, delivery of CC shall be initiated at least after every finished POP3 command/response.

B.6 POP3 Interception example

```
(C: Client/Target, S: Server/Provider, I: Intercept operation)

[01] S: <wait for connection on TCP port 110>
[02] C: <open connection>
[03] S:    +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>
[04] C:    APOP mrose c4c9334bac560ecc979e58001b3e22fb
[XX] I: Create Session [allocate CIN]
[05] S:    +OK mrose's maildrop has 2 messages (320 octets)
[XX] I: Send email-logon event with E-mail-Status OK
[XX] I: Send CC for message 4-5
[06] C:    STAT
[07] S:    +OK 2 320
[XX] I: Send CC for message 6-7
[08] C:    LIST
[09] S:    +OK 2 messages (320 octets)
[10] S:    1 120
[11] S:    2 200
[12] S:    .
[XX] I: Send CC for message 8-12
[13] C:    RETR 1
[14] S:    +OK 120 octets
[15] S:    <the POP3 server sends message 1>
[16] S:    .
[XX] I: Send email-download event
[XX] I: Send CC for message 13-16
[17] C:    DELE 1
[18] S:    +OK message 1 deleted
[XX] I: Send CC for message 17-18
[19] C:    TOP 2 10
[20] S:    +OK top of message follows

[21] S:    <the POP3 server sends first 10 lines of message 2>
[22] S:    .
[XX] I: Send email-partial-download event
[XX] I: Send CC for message 19-22
[23] C:    DELE 2
[24] S:    +OK message 2 deleted
[XX] I: Send CC for message 23-24
[25] C:    QUIT
[26] S:    +OK dewey POP3 server signing off (maildrop empty)
[XX] I: Send email-logoff event
[XX] I: Send CC for message 25-26
[XX] I: Close Session [release CIN]
[27] C: <close connection>
[28] S: <wait for next connection>
```

Annex C (normative):
IMAP4

C.1 IMAP4 introduction

IMAP version 4 (IMAP4) RFC 3501 [10] can generally be viewed as a means for remotely manipulating E-mail stored on a server in a mailbox and the mailboxes itself. Extending the capabilities of POP3, IMAP4 provides means to create, change and delete folders of the mailbox. The APPEND command provides a "send"-like facility. IMAP4 connections consist of the establishment of a client/server network connection, an initial greeting from the server, and client/server interactions. These client/server interactions consist of a client command, server data, and a server completion result response.

The LI-relevant IMAP interactions shall be represented by one or more IRI records. The complete data of all interactions shall be delivered as call content if requested.

Clause C.2 indicates which events can be expected when intercepting IMAP4 communication session(s) and provides a table mapping the LI-relevant IMAP4 commands to corresponding IRI messages.

Clause C.3 details the delivery of CC.

Clause C.4 contains an example of IMAP4 communication session and related LI events.

C.2 IMAP4 HI2 event-record mapping

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

Table C.1 details the mapping of LI-relevant IMAP4 commands and corresponding IRI events. For every execution of one of the listed commands, an IRI message of the specified type shall be sent to the LEA.

Table C.1: IMAP4 and related LI events

IMAP4 Command	Description	ASN.1 E-mail-Event	iRIType
LOGIN	login client using clear text username+password	e-mail-logon	Begin
AUTHENTICATE	authenticate client according to RFC 4422 [16] SASL	e-mail-logon	Begin
FETCH	retrieve message(s) according to specified criteria	e-mail-download	Report
	retrieve parts of message(s) according to specified criteria	e-mail-partial-download	Report
APPEND	append argument as last mail in mailbox	e-mail-upload	Report
UID FETCH	do COPY, FETCH or STORE on message(s) based on specified UID, instead of message sequence number	e-mail-download	Report
	do COPY, FETCH or STORE on part of message(s) based on specified UID, instead of message sequence number	e-mail-partial-download	Report
LOGOUT	close session	e-mail-logoff	End

NOTE 1: The UID command supports the IMAP commands FETCH, COPY and STORE on the message with the specified UID. From a LI perspective, only UID FETCH contains IRI relevant information.

NOTE 2: RFC 3501 [10] IMAP4 states "A non-existent UID is ignored without any error message generated. Thus, it is possible for a UID FETCH command to return an OK without any data". In this case, an IRI record with E-mail-Status "successful" could be generated even though no message with the specified UID exists.

IRI messages shall be sent directly after the IMAP4 interaction has been completed.

For all commands, the success of the IMAP4 command shall be indicated using the ASN.1 field E-mail-Status in the same IRI message according to table C.2.

Table C.2: Mapping of IMAP4 response and ASN.1 E-mail-Status field

IMAP 4 Response	Value of ASN.1 E-mail-Status
OK	successful
NO	failed

C.3 IMAP4 HI3 delivery of call content

The nature of IMAP4 as a message access and mailbox (folder) manipulation protocol leads to CC containing not only information directly related to E-mails, but additional information also, e.g. folder manipulation and mail status flags. Call content (CC) shall contain the complete data of all IMAP4 sessions initiated by a target. Sessions extend from LOGIN or AUTHENTICATE to LOGOUT commands. LOGIN, AUTHENTICATE and LOGOUT itself are included.

IMAP4 provides the possibility to extend individual sessions to long periods of time (theoretically up to weeks), making it impractical to deliver CC only after the session is closed. To keep the delay between original communication and delivery of CC to an amount acceptable to LEAs, delivery of CC shall be initiated at least after every finished IMAP4 interaction.

C.4 IMAP4 Interception example

(C: Client/Target, S: Server/Provider, I: Intercept operation)

```
[01] C: (Client connects to IMAP server)
[02] S: * OK IMAP4rev1 Service Ready
[03] C: a001 login mrc secret
```
[XX] I: Create Session [allocate CIN]
```
[04] S: a001 OK LOGIN completed
```
[XX] I: Send email-logon event with E-mail-Status OK
[XX] I: Send CC for message 3-4
```
[05] C: a002 select inbox
[06] S: * 18 EXISTS
[07] S: * FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
[08] S: * 2 RECENT
[09] S: * OK [UNSEEN 17] Message 17 is the first unseen message
[10] S: * OK [UIDVALIDITY 3857529045] UIDs valid
[11] S: a002 OK [READ-WRITE] SELECT completed
```
[XX] I: Send CC for message 5-11
```
[12] C: a003 fetch 12 full
[13] S: * 12 FETCH (FLAGS (\Seen) INTERNALDATE "17-Jul-1996 02:44:25 -0700"
     RFC822.SIZE 4286 ENVELOPE ("Wed, 17 Jul 1996 02:23:25 -0700 (PDT)"
     "IMAP4rev1 WG mtg summary and minutes"
     (("Terry Gray" NIL "gray" "cac.washington.edu"))
     (("Terry Gray" NIL "gray" "cac.washington.edu"))
     (("Terry Gray" NIL "gray" "cac.washington.edu"))
     ((NIL NIL "imap" "cac.washington.edu"))
     ((NIL NIL "minutes" "CNRI.Reston.VA.US")
     ("John Klensin" NIL "KLENSIN" "INFOODS.MIT.EDU")) NIL NIL
     "")
     BODY ("TEXT" "PLAIN" ("CHARSET" "US-ASCII") NIL NIL "7BIT" 3028 92))
[14] S: a003 OK FETCH completed
```
[XX] I: Send email-partial-download
[XX] I: Send CC for message 12-14
```
[15] C: a004 fetch 12 body[header]
[16] S: * 12 FETCH (BODY[HEADER] {350}
[17] S: Date: Wed, 17 Jul 1996 02:23:25 -0700 (PDT)
[18] S: From: Terry Gray
[19] S: Subject: IMAP4rev1 WG mtg summary and minutes
[20] S: To: imap@cac.washington.edu
```

```
[21] S: cc: minutes@CNRI.Reston.VA.US, John Klensin
[22] S: Message-Id:
[23] S: MIME-Version: 1.0
[24] S: Content-Type: TEXT/PLAIN; CHARSET=US-ASCII
[25] S:
[26] S: )
[27] S: a004 OK FETCH completed
```
[XX] I: Send email-partial-download
[XX] I: Send CC for message 15-27
```
[28] C: a005 store 12 +flags \deleted
[29] S: * 12 FETCH (FLAGS (\Seen \Deleted))
[30] S: a005 OK +FLAGS completed
```
[XX] I: Send CC for message 28-30
```
[31] C: a006 logout
[32] S: * BYE IMAP4rev1 server terminating connection
[33] S: a006 OK LOGOUT completed
```
[XX] I: Send email-logoff
[XX] I: Send CC for message 31-33
[XX] I: Close Session [release CIN]

Annex D (normative):
Messaging ASN.1

The ASN.1 (Recommendation ITU-T X.680 [11]) module that represents the information in the present document and meets all stated requirements is shown below. TR 102 503 [i.2] gives an overview of the relevant Object IDentifiers (OID) used in ASN.1 modules of the Lawful Intercept specifications and points to the specification where the modules can be found.

The ASN.1 definitions are in .txt file "EmailPDU,ver12.txt", contained in archive ts_10223202v030601p0.zip which accompanies the present document.

    NOTE: The term "EmailPDU" instead of "MessagingPDU" is used for reasons of backwards compatibility.

```
-- ===========================
-- Description of the Email PDU
-- ===========================

EmailPDU
{itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5) email(2)
version12(12)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
IMPORTS

    -- from TS 101 671 [4]
    IPAddress
        FROM HI2Operations
        {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) hi2(1)
version17(17)}

    -- from TS 102 232-5 [38]
    IPMMCC
        FROM IPMultimediaPDU
        {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulIntercept(2) li-ps(5)
iPMultimedia(5) version6(6)};
```

```
-- ===========================
-- Object Identifier Definition
-- ===========================

emailIRIObjId RELATIVE-OID        ::= {li-ps(5) email(2) version12(12) iRI(1)}
emailCCObjId RELATIVE-OID         ::= {li-ps(5) email(2) version12(12) cC(2)}
messagingIRIObjId RELATIVE-OID  ::= {li-ps(5) email(2) version12(12) messagingIRI(3)}
messagingCCObjId RELATIVE-OID   ::= {li-ps(5) email(2) version12(12) messagingCC(4)}
messagingMMCCObjId RELATIVE-OID ::= {li-ps(5) email(2) version12(12) messagingMMCC(5)}

    -- definitions are relative to
    -- {itu-t(0) identified-organization(4) etsi(0) securityDomain(2) lawfulintercept(2)}
```

```
-- ===========================
-- Email Communications Contents
-- ===========================
```

```
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
}
```

```
-- ====================================
-- Intercept-related information for Email
-- ====================================
```

```
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)) OPTIONAL,
        -- Not available in some cases; if a value is available, it shall be provided
    e-mail-Recipients        [10] E-mail-Address-List OPTIONAL,
        -- Not available in some cases; if a value is available, it shall be provided
    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
    ...,
    national-EM-ASN1parameters [15] National-EM-ASN1parameters OPTIONAL,
        -- Completely defined on a national basis
    aAAInformation           [16] AAAInformation OPTIONAL,
    e-mail-Sender-Validity   [17] ENUMERATED
        {
            validated(0),
                -- The operator has assured the e-mail-sender
            nonvalidated(1),
                -- The operator does not assure the e-mail-sender
            ...
        } OPTIONAL
}
```

```
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-logon-attempt(4),
    e-mail-logon(5),
    e-mail-logon-failure(6),
    e-mail-logoff(7),
    e-mail-partial-download(8),
    e-mail-upload(9)
}
```

```
E-mail-Protocol ::= ENUMERATED
```

```
{
    smtp(1),
    pop3(2),
    imap4(3),
    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))
```

```
National-EM-ASN1parameters ::= SEQUENCE
{
    countryCode     [1] PrintableString (SIZE (2)),
        -- Country Code according to ISO 3166-1 [12],
        -- the country to which the parameters inserted after the extension marker apply
    ...
        -- In case a given country wants to use additional national parameters according to its law,
        -- these national parameters should be defined using the ASN.1 syntax and added after the
        -- extension marker (...)
}
```

```
AAAInformation ::= CHOICE
    -- The AAAInformation field allows for POP3 and authenticated SMTP AAA information
{
    pOP3AAAInformation          [0] POP3AAAInformation,
    aSMTPAAAInformation         [1] ASMTPAAAInformation,
    ...,
    iMAPAAAInformation          [2] IMAPAAAInformation
}
```

```
POP3AAAInformation ::= SEQUENCE
    -- The POP3AAAInformation field contains the POP3 username & optionally the password
{
    username                    [0] UTF8String (SIZE (0..64)),
    password                    [1] UTF8String (SIZE (0..64)) OPTIONAL,
    aAAResult                   [2] AAAResult OPTIONAL,
    ...
}
```

```
ASMTPAAAInformation ::= SEQUENCE
    -- The ASMTPAAAInformation field contains the SMTP username and
    -- optionally the authentication fields
{
    username                    [0] UTF8String (SIZE (0..64)),
    authMethod                  [1] AAAauthMethod OPTIONAL,
        -- The hashing method used, i.e. CRAM-MD5, DIGEST-MD5, etc
    challenge                   [2] OCTET STRING OPTIONAL,
        -- A BASE64 encoded challenge send by the SMTP server
    response                    [3] OCTET STRING OPTIONAL,
        -- A BASE64 encoded hashed response returned by the client
    aAAResult                   [4] AAAResult OPTIONAL,
    ...
}
```

```
IMAPAAAInformation ::= SEQUENCE
    --- The iMAPAAAInformation field contains the IMAP username & optionally the password
{
    username                    [0] UTF8String (SIZE (0..64)),
    password                    [1] UTF8String (SIZE (0..64)) OPTIONAL,
    aAAResult                   [2] AAAResult OPTIONAL,
    ...
}
```

```
AAAResult ::= ENUMERATED
{
    resultUnknown(1),
    aAAFailed(2),
    aAASucceeded(3),
    ...
}
```

ETSI

```
AAAauthMethod ::= ENUMERATED
{
    undefinedAuthMethod(1),
    cramMD5(2),
    digestMD5(3),
    ...
}
```

```
-- ===============================
-- Messaging Communications Contents
-- ===============================
```

```
MessagingCC ::= SEQUENCE
    -- MessagingCC is the PDU sent for the captured content
{
    messaging-cc-obj-id         [0] RELATIVE-OID,
    event-identifier            [1] INTEGER (0..4294967295),
        -- Used to correlate to MessagingIRI within the same CIN
    content-identifier          [2] INTEGER (0..4294967295) OPTIONAL,
    sequence-number             [3] INTEGER (0..4294967295) OPTIONAL,
    end-of-sequence             [4] BOOLEAN DEFAULT FALSE,
    content-type                [5] OCTET STRING,
        -- MIME content type, i.e.: image/png, text/plain;charset=utf8, audio/PCMA
    content                     [6] OCTET STRING,
    ...
}
```

```
MessagingMMCC ::= SEQUENCE
    -- MessagingMMCC is the PDU sent for the captured IPMMCC content
{
    messaging-mm-cc-obj-id      [0] RELATIVE-OID,
    event-identifier            [1] INTEGER (0..4294967295),
        -- Used to correlate to MessagingIRI within the same CIN
    content-identifier          [2] INTEGER (0..4294967295) OPTIONAL,
    content                     [3] IPMMCC,
    ...
}
```

```
-- =========================================
-- Intercept-related information for Messaging
-- =========================================
```

```
MessagingIRI ::= SEQUENCE
{
    messaging-iri-obj-id        [0] RELATIVE-OID,
    system-type                 [1] Messaging-System-Type,
    system-identifier           [2] OCTET STRING OPTIONAL,
        -- Identifier up to national agreement, uniquely identifies a certain messaging system
    category                    [3] Messaging-Event-Category OPTIONAL,
    status                      [4] Messaging-Status,
    party-information           [5] SET OF Messaging-Party-Information OPTIONAL,
    trigger                     [6] Messaging-Trigger,
    properties                  [7] SEQUENCE OF Messaging-Property OPTIONAL,
    event-identifier            [8] INTEGER (0..4294967295) OPTIONAL,
        -- Used to correlate to MessagingCC or MessagingMMCC within the same CIN. Mandatory when CC
is also sent
    original-message            [9] OCTET STRING OPTIONAL,
    ...,
    box-identifier              [10] OCTET STRING OPTIONAL
}
```

```
Messaging-System-Type ::= ENUMERATED
{
    unified-messaging(1),
    ...
}
```

```
Messaging-Event-Category ::= CHOICE
{
    message                       [0] Messaging-Event,
    message-box                   [1] Messaging-Box-Event,
    message-notification          [2] Messaging-Notification-Event,
    call                          [3] Messaging-Call-Event,
    ...
}
```

```
Messaging-Event ::= ENUMERATED
{
    deposit(1),
    retrieve(2),
    delete(3),
    save(4),
    slamdown(5),
    ...
}
```

```
Messaging-Box-Event ::= ENUMERATED
{
    login(1),
    logout(2),
    lock(3),
    unlock(4),
    activate(5),
    deactivate(6),
    delete(7),
    pin-change(8),
    greeting-record(9),
    greeting-change(10),
    greeting-delete(11),
    greeting-enable(12),
    greeting-disable(13),
    notification-enable(14),
    notification-disable(15),
    disconnect(16),
    connect(17),
    ...,
    greeting-play(18),
    language-change(19),
    pin-security-enable(20),
    pin-security-disable(21)
}
```

```
Messaging-Notification-Event ::= ENUMERATED
{
    sms(1),
    sms-deposit(2),
    sms-slamdown(3),
    sms-pin-reminder(4),
    email(5),
    fax-to-email(6),
    ...,
    mms(7)
}
```

```
Messaging-Call-Event ::= ENUMERATED
{
    callout(1),
    ...
}
```

```
Messaging-Status ::= ENUMERATED
{
    unknown(0),
    not-applicable(1),
    operation-failed(2),
    operation-succeeded(3),
    operation-cancelled(4),
    operation-started(5),
    ...,
    operation-lost(6)
}
```

```
Messaging-Party-Information ::= SEQUENCE
{
    party-qualifier      [0] Messaging-Party-Qualifier,
    party-identity       [1] Messaging-Party-Identity,
    ...,
    party-validity       [2] Messaging-Party-Validity OPTIONAL,
    copy-qualifier       [3] Messaging-Copy-Qualifier OPTIONAL
}
```

```
Messaging-Party-Qualifier ::= ENUMERATED
{
    unknown-party(0),
        -- In this case the party cannot be classified as either originating or terminating
    originating-party(1),
        -- In this case, the partyInformation parameter provides the identities related to
        -- the originating party and all information provided by this party.
    terminating-party(2),
        -- In this case, the partyInformation parameter provides the identities related to
        -- the terminating party and all information provided by this party.
    ...,
    associated-party(3)
        -- In this case, the partyInformation parameter provides the identities related to
        -- an associated party and all information provided by this party.
}
```

```
Messaging-Party-Identity ::= CHOICE
{
    msisdn             [0] OCTET STRING (SIZE (1..9)),
        -- MSISDN of the target, encoded in the same format as the AddressString
        -- parameters defined in MAP format 3GPP TS 09.02 [22], clause 17.7.8.
    e164-format        [1] OCTET STRING (SIZE (1..25)),
        -- E.164 address of the node in international format. Coded in the same format as
        -- the calling party number parameter of the ISUP (parameter part: EN 300 356 [23])
    email-address      [2] E-mail-Address-List,
    ...,
    ip-address         [3] IPAddress,
        --IPAddress is defined by IETF RFC 791 [31] and RFC 2460 [34]
    alphanumeric       [4] UTF8String,
    ip-address-and-port [5] IP-Address-And-Port,
    imsi               [6] OCTET STRING (SIZE (3..8)),
        -- International Mobile Subscriber Identity of the target, encoded in the same format as the
        -- TBCD-STRING parameter defined in MAP format 3GPP TS 29.002 [36], clause 17.7.8.
        -- It is described in 3GPP TS 23.003 [37] clause 2.2.
    imei               [7] OCTET STRING (SIZE (8)),
        -- International Mobile Equipment Identity of the target, encoded in the same format as the
        -- TBCD-STRING parameter defined in MAP format 3GPP TS 29.002 [36], clause 17.7.8.
        -- It is defined in 3GPP TS 23.003 [37] clause 6.
    fax-url            [8] OCTET STRING,
        -- see format defined in RFC 2806 [29].
    tel-url            [9] OCTET STRING,
        -- see format used in 3GPP TS 33.108 [5], 3GPP TS 24.229 [30] and defined in RFC 2806 [29].
    modem-url          [10] OCTET STRING,
        -- see format defined in RFC 2806 [29].
    sip-uri            [11] OCTET STRING,
        -- see format used in in 3GPP TS 33.108 [5] and defined in RFC 3261 [32].
    sips-uri           [12] OCTET STRING,
        -- see format defined in RFC 3261 [32].
    nai                [13] OCTET STRING
        -- Network Access Identity of the party, encoded in the same format as used EPS
        -- domain in 3GPP TS 33.108 [5] and defined in RFC 4282 [33].
}
```

```
IP-Address-And-Port ::= SEQUENCE
{
    ip-address             [0] IPAddress,
        -- IPAddress is defined by IETF RFC 791 [31] and RFC 2460 [34]
    port-number            [1] INTEGER,
        -- port-number is defined by IETF RFC 6335 [35]
    ...
}
```

```
Messaging-Party-Validity ::= ENUMERATED
{
    unknown(0),
    trusted(1),
    untrusted(2),
    ...
}
```

```
Messaging-Copy-Qualifier ::= ENUMERATED
{
    unknown(0),
    none(1),
    cc(2),
    bcc(3),
    ...
}
```

```
Messaging-Trigger ::= ENUMERATED
{
    unknown(0),
    user(1),
    user-agent(2),
    system(3),
    system-operator(4),
    ...
}
```

```
Messaging-Property ::= CHOICE
{
    pincode            [0] OCTET STRING (SIZE (1..32)),
    ...,
    priority           [1] Messaging-Property-Priority,
    greeting-type      [2] Messaging-Property-Greeting-Type,
    notification-type  [3] Messaging-Property-Notification-Type,
    language           [4] OCTET STRING,
        -- Language according to RFC 3066 [24]
    message-identifier [5] OCTET STRING,
    subject            [6] UTF8String,
    user-agent         [7] UTF8String,
    password           [8] OCTET STRING,
    message-status     [9] Messaging-Property-Message-Status,
    requested-reports  [10] Messaging-Property-Requested-Reports,
    expires            [11] GeneralizedTime,
    message-date       [12] GeneralizedTime
}
```

```
Messaging-Property-Priority ::= ENUMERATED
{
    low(1),
    medium(2),
    high(3),
    private(4),
    ...
}
```

```
Messaging-Property-Greeting-Type ::= ENUMERATED
{
    general(1),
    name(2),
    personal(3),
    absence(4),
    number(5),
    ...
}
```

```
Messaging-Property-Notification-Type ::= ENUMERATED
{
    empty-call(1),
    lost-call(2),
    ...,
    message-to-email(3),
    read-report(4),
    delivery-report(5),
    allow-delivery-report(6),
    deny-delivery-report(7)
}
```

```
Messaging-Property-Message-Status ::= ENUMERATED
{
    indeterminate(0),
    expired(1),
    retrieved(2),
    rejected(3),
    deferred(4),
    forwarded(5),
    unrecognized(6),
    unreachable(7),
    read(8),
    deleted-without-being-read(9),
    delivery-condition-not-met(10),
    ...
}
```

```
Messaging-Property-Requested-Reports ::= ENUMERATED
{
    none(0),
    delivery(1),
    read(2),
    delivery-and-read(3),
    ...
}
```

```
END -- end of EmailPDU
```

Annex E (informative):
E-mail LI requirements

E.1 HI2 requirements

[E.1.1] The HI2 interface has to 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 has to 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 has to 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 the ability to transfer both addresses is supported.

[E.1.4] When HI2 is able to deliver an E-mail address, either sender or receiver, the MF has not to 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 has to 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 TOs. Since there is no expectation that the intercept device or the MF have unlimited resources we 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 TOs, and provide for a means to notify the LEA that we hit this condition.

[E.1.6] The RFC 5322 [7] E-mail message envelope fields of dates, source, and destination may be considered IRI. These fields are defined in RFC 5322 [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 has to 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 has to 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 has to 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 has to also contain the results of the logon attempt.

NOTE 9:   This has been required by LEAs.

[E.1.10]   The HI2 interface has to 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 has to 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 has to support the ability to deliver the Message-ID.

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

[E.1.13]   The authentication data resulting from either sending or downloading E-mail, has to be part of IRI in the case of application layer intercept. In the case of IP-packet interception, requirement [E.2.3] applies.

NOTE 12:   The choice between options is depending on implementation and subject to agreement between LEA and CSP.

E.2   HI3 requirements

[E.2.1]   HI3 delivery of E-mail content has to include the entire E-mail message body. See RFC 5322 [7] for a definition of the body.

NOTE 1: Anything less would be incomplete data.

[E.2.2]   HI3 delivery of E-mail content has to include the entire E-mail envelope, when applicable. See RFC 5322 [7] for a definition of the envelope.

NOTE 2: The RFC 5322 [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]   In the case of IP packet interception, the authentication data resulting from either sending or downloading E-mail, has to be sent as part of HI3, in the form of the IP packets exchanged in the authentication. In the case of application layer interception, requirement [E.1.13] applies.

NOTE 3: The choice between options is depending on implementation and subject to agreement between LEA and provider.

[E.2.4]   The RFC 5322 [7] E-mail message body has to 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 5322 [7] E-mail message envelope fields that are declared optional in RFC 5322 [7] have to 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 has to 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 HI3 has to 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 has to be called "IP-packet" delivery.

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

[E.2.8]   E-mail HI3 has to 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 has to 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.

  NOTE 9:   In the case of IP packet interception, the use of features such as STARTTLS, as defined in RFC 3207 [17] for SMTP and RFC 2595 [18] and RFC 4616 [19] for POP3 and IMAP, prohibit meeting the requirements defined in clauses E.1 and E.2 if the decryption key is not made available.

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.1.13]	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
[E.2.4]	6.2.3, 6.3.3, 6.4.3
[E.2.5]	6.2.3, 6.3.3, 6.4.3
[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-mails from one host computer to another. The remaining text below is based on ideas expressed in RFC 5321 [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 5321 [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 without 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 5321 [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 5321 [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). The fact that a SMTP address may be spoofed can be signalled using the ASN.1 e-mail-Sender-Validity structure. In some cases the user has to authenticate before accessing the service. In this case the validity is available.

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 has to 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 5322 [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.
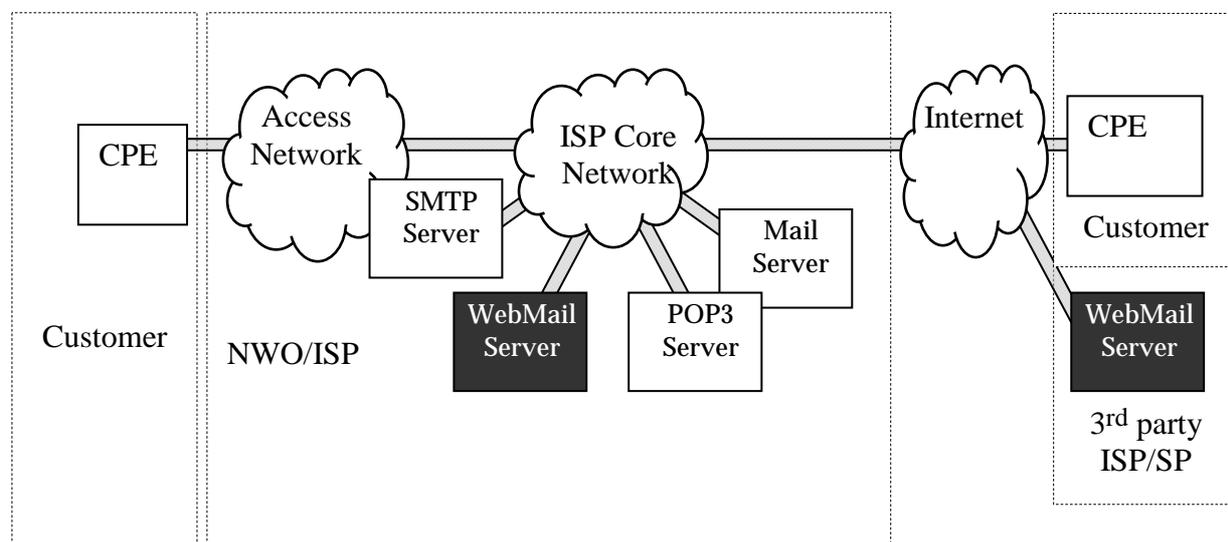
Figure H.1: Webmail network topology

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.
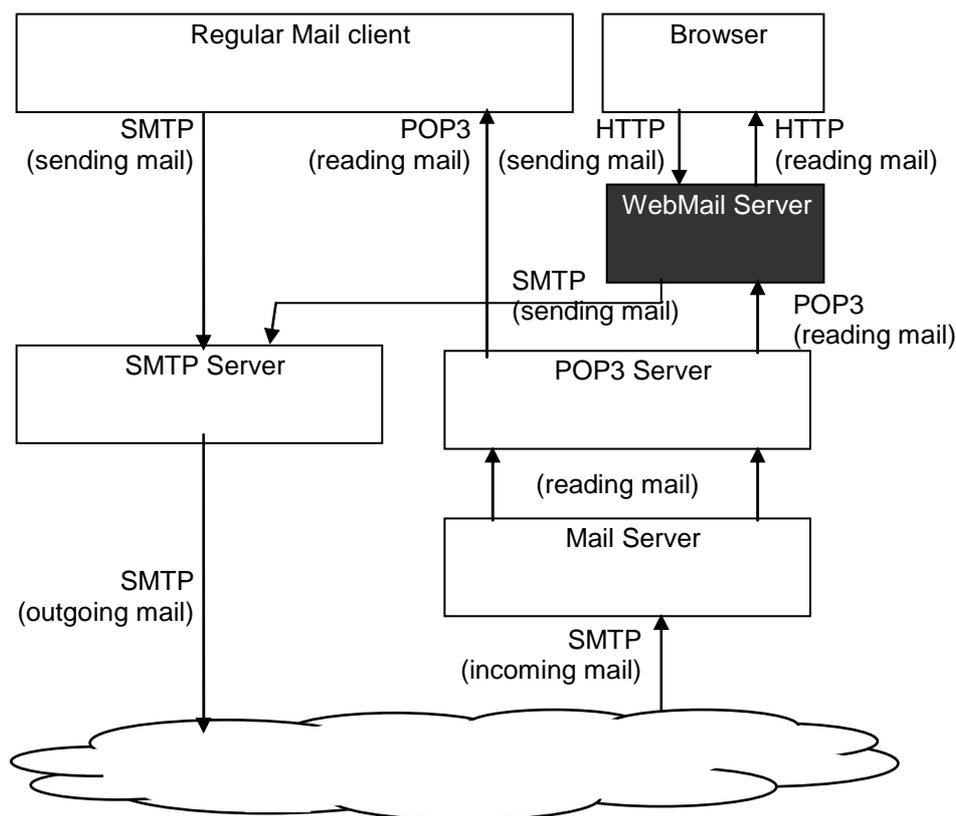
Figure H.2: Webmail protocols

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.
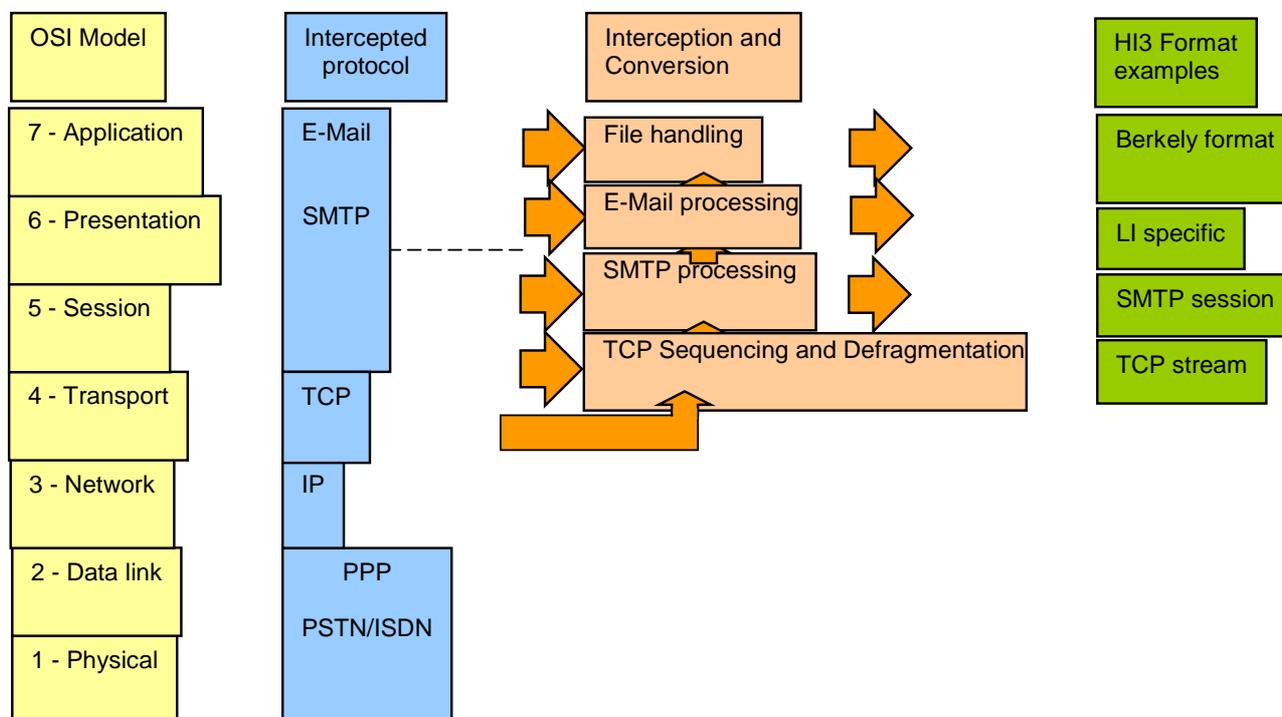

Figure I.1: Discussion diagram

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 have to 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 has to 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 (see 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 have to be discussed, before one or more HI3 formats can be selected.

Annex J (informative):
Change Request History

Status of Technical Specification TS 102 232-2 Service-specific details for messaging services		
TC LI approval date	**Version**	**Remarks**
January 2004	1.1.1 TS 102 233	First publication of TS 102 233 after ETSI/TC LI#04 (14-16 October 2003, Moscow) approval Version 1.1.1 prepared by Jon Sjoberg (Top Layer) (rapporteur)
April 2004	1.2.1 TS 102 233	Included Change Requests: TS102233CR001r1 (cat B) Introduction of an ASN.1 type for national ASN.1 coded parameters in the ASN.1 module This CR was approved by TC LI#05 (23-25 March 2004, Oxford) Version 1.2.1 prepared by Peter van der Arend (KPN) (chairman TC LI)
May 2006	1.3.1 TS 102 233	Included Change Requests: TS102233CR002r1 (cat B) partial download of e-mail TS102233CR003r1 (cat B) Send username and password in HI2 These CRs were approved by TC LI#12 (9-11 may 2006, Limassol) Version 1.3.1 prepared by Mark Lastdrager (Pine Digital Security) (rapporteur)
September 2006	2.1.1	Included Change Requests: TS102233CR004 (cat B) IMAP interception TS102233CR005 (cat D) Updates of notes These CRs were approved by TC LI#13 (6-8 September 2006, Stockholm) **TS 102 233 is converted to <u>part 02</u> of the multi part specification TS 102 232** Version 2.1.1 prepared by Peter van der Arend (KPN) (chairman TC LI) Rapporteur of this specification is Mark Lastdrager (Pine Digital Security)
April 2007	2.2.1	Included Change Requests: TS102232-02CR006 (cat F) Message ID for SMTP part of the specification TS102232-02CR007r1 (cat F) Message ID for POP3 part of the specification These CRs were approved by TC LI#15 (23-25 April 2007, Riga) Version 2.2.1 prepared by Peter van der Arend (KPN) (chairman TC LI)
October 2007	2.3.1	Included Change Requests: TS102232-02CR008 (cat B) Add 'e-mail-upload' to E-Mail-Event TS102232-02CR009 (cat B) Add 'imap4' to E-Mail-Protocol TS102232-02CR010r1 (cat D) Clarification on the use of TLS or SSL-based transports for email These CRs were approved by TC LI#16 (2-4 October 2007, Berlin) Version 2.3.1 prepared by Peter van der Arend (KPN) (chairman TC LI)
July 2009	2.4.1	Included Change Request: TS102232-02CR011 (cat B) Additions for POP3 interception This CR was approved by TC LI#21 (29 June - 1 July 2009, Sophia Antipolis) The ASN.1 definitions are contained in an .asn file (TS 102 232-2, EmailPDU, ver4.asn) which accompanies the present document Version 2.4.1 prepared by Peter van der Arend (Vodafone) (chairman TC LI) Rapporteur of this specification is Mark Lastdrager (Pine Digital Security)

Status of Technical Specification TS 102 232-2 Service-specific details for messaging services		
TC LI approval date	Version	Remarks
June 2010	2.5.1	Included Change Requests: TS102232-02CR012 (cat B) Addition of IMAP "AAA" Information This CR was approved by TC LI#23 (9-11 February 2010, Rome) TS102232-02CR013r1 (cat D) Modifications of IETF RCF references TS102232-02CR014r1 (cat D) Informative annex E is containing normative requirements These CRs were approved by TC LI#24 (15-17 June 2010, Aachen) The ASN.1 definitions are contained in a .txt file (TS 102 232-2, EmailPDU, ver5.txt) which accompanies the present document Version 2.5.1 prepared by Peter van der Arend (Vodafone) (chairman TC LI) Rapporteur of this specification is Mark Lastdrager (Pine Digital Security)
June 2011	2.6.1	Included Change Request: TS102232-02CR015r1 (cat B) Addition of Party-validity to IRI This CR was approved by TC LI#27 (28-30 June 2011; Mariehamn) The ASN.1 definitions are contained in a .txt file (EmailPDU,ver6.txt) which accompanies the present document Version 2.6.1 prepared by Peter van der Arend (Vodafone) (chairman TC LI)
January 2012	3.1.1	Included Change Request: TS102232-02CR016r2 (cat B) Extension with handover of messaging services This CR was approved by TC LI#29 (24-26 January 2012, Dun Laoghaire) **Title is changed from "Service-specific details for e-mail services" to "Service-specific details for messaging services". Edition 3 is created of the multi part specification TS 102 232** The ASN.1 definitions are contained in a .txt file (EmailPDU,ver7.txt) which accompanies the present document Version 3.1.1 prepared by Peter van der Arend (Vodafone) (chairman TC LI) Rapporteur of this specification is Mark Lastdrager (Pine Digital Security)
May 2012	3.2.1	Included Change Request: TS102232-02CR017r2 (cat F) Improvements to new Unified Messaging contents This CR was approved by TC LI#30 (14-16 May 2012, Amsterdam) The ASN.1 definitions are contained in a .txt file (EmailPDU,ver8.txt) which accompanies the present document Version 3.2.1 prepared by Peter van der Arend (Vodafone) (chairman TC LI) Rapporteur of this specification is Mark Lastdrager (Pine Lawful Interception)
September 2012	3.3.1	Included Change Request: TS102232-02CR018r2 (cat C) Further improvements of Unified Messaging handover This CR was approved by TC LI#31 (25-27 September 2012, Split) The ASN.1 definitions are contained in a .txt file (EmailPDU,ver9.txt) which accompanies the present document Version 3.3.1 prepared by Peter van der Arend (Vodafone) (chairman TC LI) Rapporteur of this specification is Mark Lastdrager (Pine Lawful Interception)
February 2013	3.4.1	Included Change Requests: TS102232-02CR020r4 (cat B) Further improvements of Unified Messaging handover (new party-identities) TS102232-02CR019 (cat B) Improvement to Unified Messaging handover These CRs were approved by TC LI#32 (14-16 January 2013, Sophia Antipolis) The ASN.1 definitions are contained in a .txt file (EmailPDU,ver10.txt) which accompanies the present document Version 3.4.1 prepared by rapporteur Mark Lastdrager (Pine Lawful Interception)

Status of Technical Specification TS 102 232-2 Service-specific details for messaging services		
TC LI approval date	**Version**	**Remarks**
July 2013	3.5.1	Included Change Requests: CR021 (Extending the signaling capabilities within Unified Messaging handover) CR022 (Update and improve references to 3GPP standards) These CRs were approved by TC LI#33 The ASN.1 definitions are contained in a .txt file (EmailPDU,ver11.txt) which accompanies the present document Version 3.5.1 prepared by rapporteur Mark Lastdrager (Pine Lawful Interception)
September 2013	3.6.1	Included Change Requests: CR023 (Adding streaming multimedia support to Unified Messaging) This CR was approved by TC LI#34 The ASN.1 definitions are contained in a .txt file (EmailPDU,ver12.txt) which accompanies the present document Version 3.6.1 prepared by rapporteur Mark Lastdrager (Pine Lawful Interception)

Annex K (informative):
Bibliography

ETSI TS 122 016: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; International Mobile station Equipment Identities (IMEI) (3GPP TS 22.016)".

History

Document history		
V1.1.1	February 2004	Publication as TS 102 233 (Historical)
V1.2.1	May 2004	Publication as TS 102 233 (Historical)
V1.3.1	September 2006	Publication as TS 102 233 (Historical)
V2.1.1	December 2006	Publication
V2.2.1	May 2007	Publication
V2.3.1	November 2007	Publication
V2.4.1	October 2009	Publication
V2.5.1	August 2010	Publication
V2.6.1	August 2011	Publication
V3.1.1	February 2012	Publication
V3.2.1	June 2012	Publication
V3.3.1	November 2012	Publication
V3.4.1	February 2013	Publication
V3.5.1	July 2013	Publication
V3.6.1	October 2013	Publication