ETSI TS 102 232-2 V3.11.1 (2017-11)

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

Reference

RTS/LI-00150-2

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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

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 (https://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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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 ETSI 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 ETSI 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], ETSI TS 101 671 [4], ETSI TS 101 331 [1] and ETSI TR 101 944 [i.1].

2 References

2.1 Normative 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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://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.

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 ETSI TS 101 671 is published as ETSI 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 4646: "Tags for Identifying 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 7542: "The Network Access Identifier".

[34] IETF RFC 8200: "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".

[39] IETF RFC 5545: "Internet Calendaring and Scheduling Core Object Specification (iCalendar)".

[40] IETF RFC 6350: "vCard Format Specification ".

[41] IETF RFC 4791: "Calendaring Extensions to WebDAV (CalDAV)".

[42] IETF RFC 6352: "CardDAV: vCard Extensions to Web Distributed Authoring and Versioning (WebDAV)".

2.2 Informative 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 referenced document (including any amendments) applies.

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

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 IETF RFC 5322 [7], clause 6.

IMAP4: protocol used to manipulate mailbox parameters on a server

NOTE: As described in IETF 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 IETF 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 IETF 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
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
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
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 IETF 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 IETF 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 3GPP TS 33.108 [5]. However if the target accesses his mailbox from a public terminal (using a PIN code), the access event is in the 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. Subject to national agreement, this requirement may be over-ridden and the handover of intercepted e-mail may use the MessagingIRI and MessagingCC or MessagingMMCC 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.

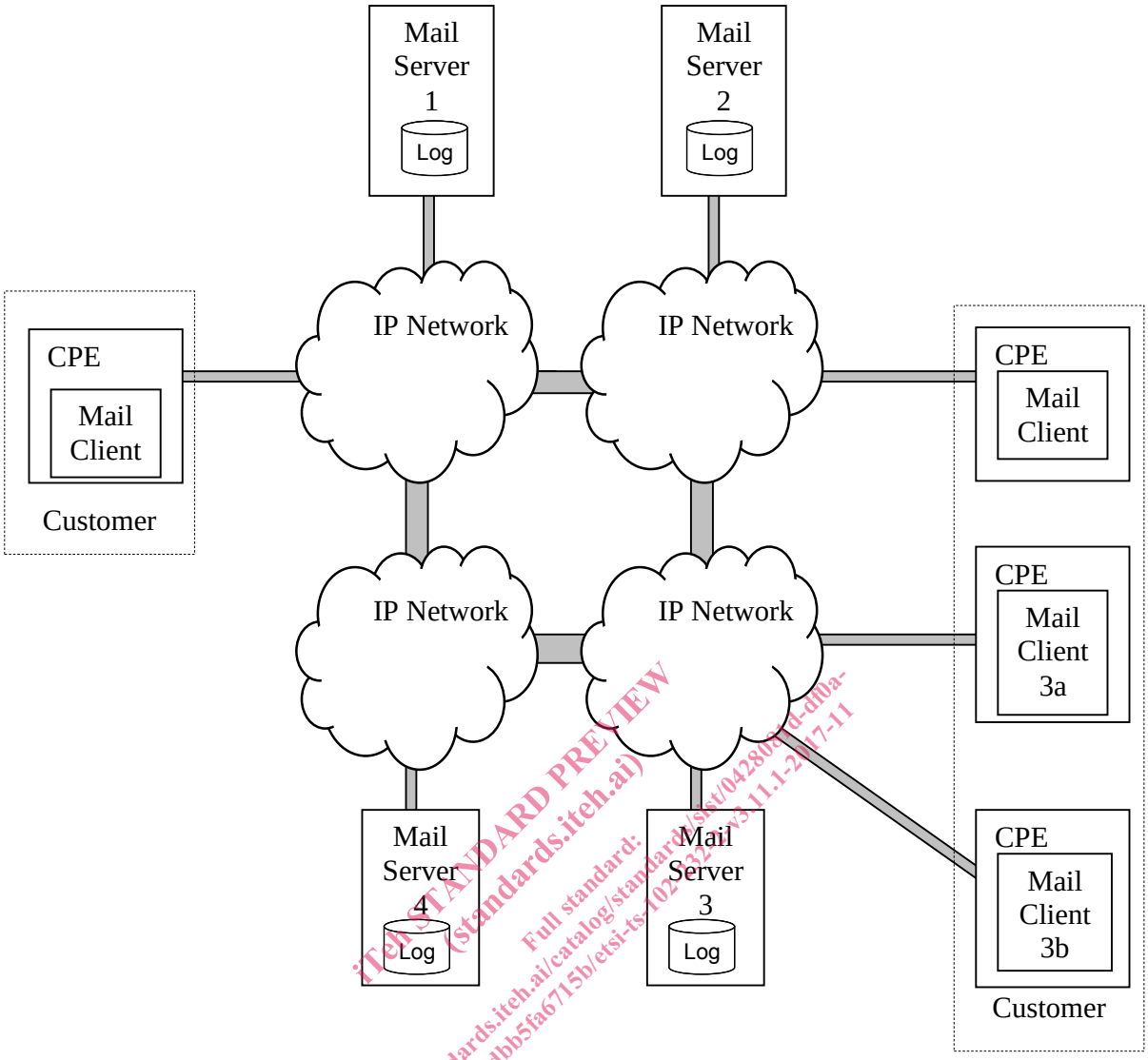

Figure 1: Reference network topology

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.

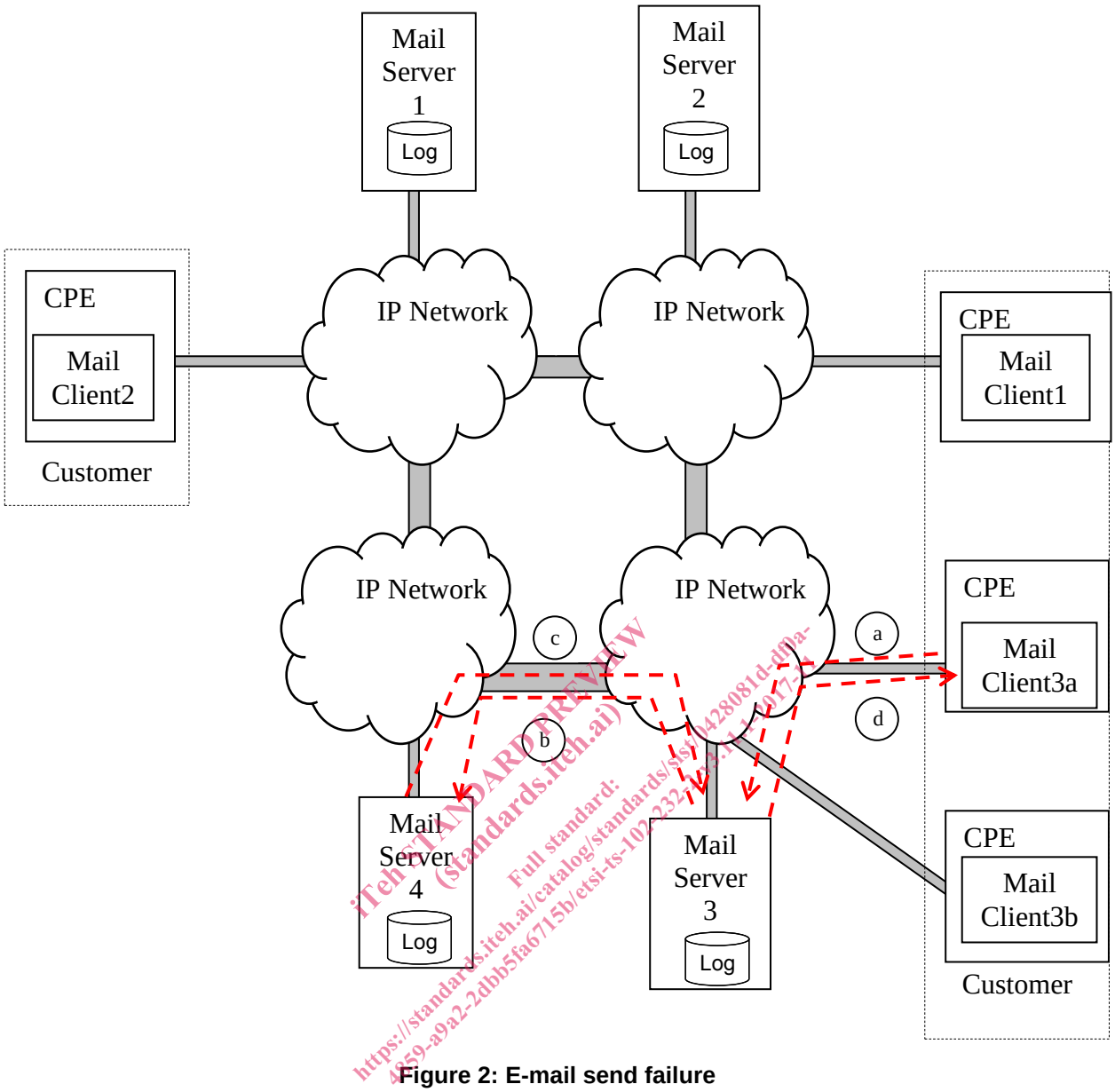

Figure 2: E-mail send failure

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 client's 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.