SLOVENSKI STANDARD
SIST-TS ETSI/TS 102 233 V1.2.1:2005

01-maj-2005

Zakonito prestrezanje (LI) ï Storitveno-specifiļne podrobnosti za storitve elektronske poģte

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

Ta slovenski standard je istoveten z: **TS 102 233 Version 1.2.1**

ICS:

33.020	Telekomunikacije na splošno	Telecommunications in general

SIST-TS ETSI/TS 102 233 V1.2.1:2005 **en**

ETSI TS 102 233 V1.2.1 (2004-05)

Technical Specification

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

Reference
RTS/LI-00012

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

ETSI

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

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

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

Important notice

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

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

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

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

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

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

Introduction

The present document describes what information is required for the handover of intercepted IP-based E-mail traffic from a 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 [3].

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

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

1 Scope

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

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

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

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

2 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 Definitions and abbreviations

3.1 Definitions

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

E-mail Address: ARPANET E-mail address

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

IMAP4: protocol used to manipulate mailbox parameters on a server

NOTE: Described in RFC 3501 [10].

mailbox: destination point of E-mail messages

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

NOTE: Described in RFC 1939 [8].

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

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

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

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

NOTE: Each E-mail contains only one sender.

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

NOTE: Described in RFC 2821 [9].

3.2 Abbreviations

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

APOP	POP3 authentication message
ASN.1	Abstract Syntax Notation One
CC	Content of Communication
CPE	Customer Premises Equipment
HI2	Handover Interface port 2 (for Intercept Related Information)
HI3	Handover Interface port 3 (for Content of Communication)
HTTP	Hyper Text Transfer Protocol
IMAP4	Internet Message Access Protocol version 4
IP	Internet Protocol
IRI	Intercept Related Information
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LEA	Law Enforcement Agency
LEMF	Law Enforcement Monitoring Facility
MF	Mediation Function
MTA	Mail Transfer Agents
NWO	Network Operator
POP3	Post-Office Protocol version 3
PSTN	Public Switched Telecommunication Network

RETR	POP3 Retrieve message
SMTP	Simple Mail Transfer Protocol
SP	Service Provider
TCP	Transmission Control Protocol

4 General

4.1 E-mail services

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

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

E-mail service, in general, can be divided into two categories: those services which allow a computer to transfer a message to another computer; and those services which allow users to manipulate their mailbox by doing such things as downloading messages from the mailbox and deleting messages from the mailbox. Both of these categories of E-mail services can be of interest to 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 0822 [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.

5 System model

5.1 Reference network topology

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

- The term "Mail Server" is used to represent a logical entity that relays mail for its mail clients, receives and (temporarily) stores mail for its mail clients, and allows mail clients access to the aforementioned stored mail and the ability to delete it from the mail server.
- The term "Mail Client" is used to represent a logical entity that either injects mail into the network 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.

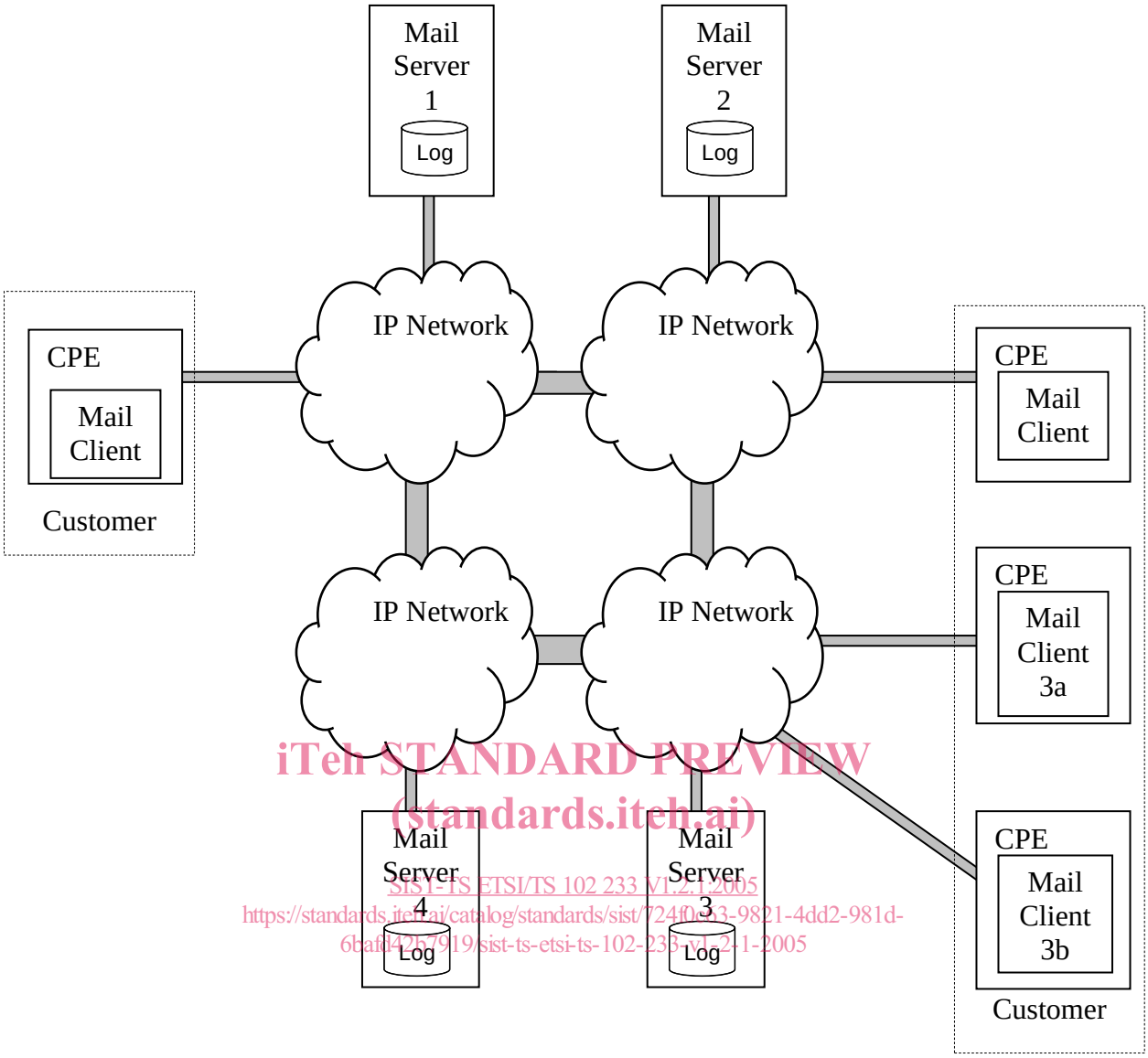

Figure 1: Reference network topology

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.

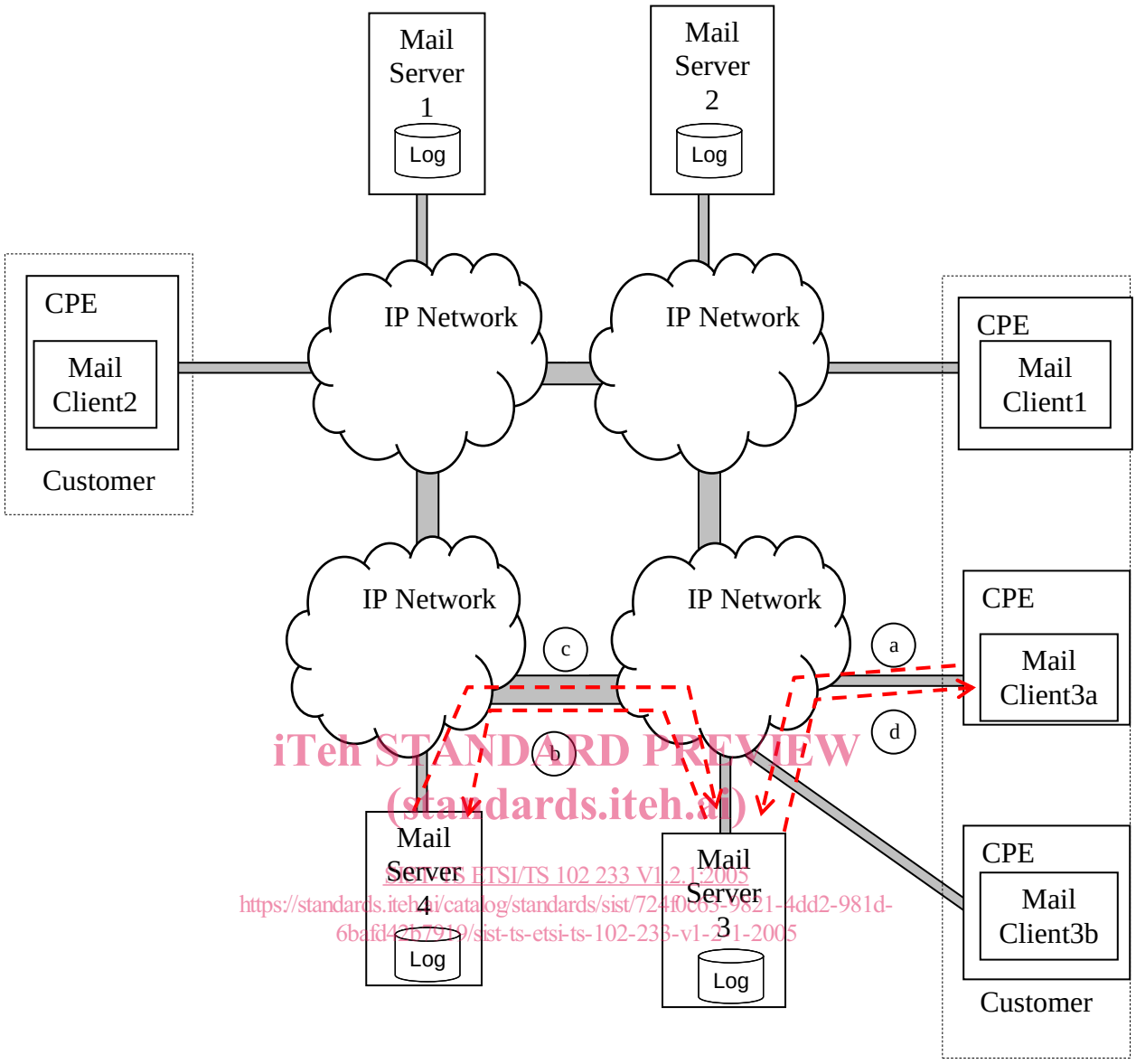

Figure 2: E-mail send failure

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.